DOES AMERICA NEED A NATIONAL IDENTIFIER?

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

NOVEMBER 16, 2001

Serial No. 107–118

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE
82–171 PDF WASHINGTON : 2002

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. McHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
MARK E. SOUDER, Indiana
STEVEN C. LaTOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. “BUTCH” OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, Jr., Tennessee

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

BERNARD SANDERS, Vermont (Independent)

Kevin Binger, *Staff Director*
Daniel R. Moll, *Deputy Staff Director*
James C. Wilson, *Chief Counsel*
Robert A. Briggs, *Chief Clerk*
Phil Schiliro, *Minority Staff Director*

Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

STEPHEN HORN, California, *Chairman*

RON LEWIS, Kentucky
DAN MILLER, Florida
DOUG OSE, California
ADAM H. PUTNAM, Florida

JANICE D. SCHAKOWSKY, Illinois
MAJOR R. OWENS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York

Ex Officio

DAN BURTON, Indiana
HENRY A. WAXMAN, California

J. Russell George, *Staff Director and Chief Counsel*
Darin Chidsey, *Professional Staff Member*
Mark Johnson, *Clerk*
David McMillen, *Minority Professional Staff Member*

CONTENTS

DOES AMERICA NEED A NATIONAL IDENTIFIER?

FRIDAY, NOVEMBER 16, 2001

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL
MANAGEMENT AND INTERGOVERNMENTAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:01 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn, Miller, Schakowsky, Owens, and Maloney.

Also present: Representative Castle.

Staff present: J. Russell George, staff director and chief counsel; Bonnie Heald, deputy staff director; Darin Chidsey and Earl Pierce, professional staff members; Mark Johnson, clerk; Jim Holms, intern; David McMillen, minority professional staff member; and Jean Gosa, minority assistant clerk.

Mr. HORN. A quorum being present, the hearing of the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations will come to order. Only 2 months after the devastating terrorist attacks of September 11, this Nation is just beginning to understand the dimensions of a dramatically changing world. Preserving the American way of life requires adaptation and sacrifice. It means using this Nation's unique strengths to address the vulnerabilities that terrorists exploited at an enormous human toll.

Technology is one of America's greatest strengths. In recent weeks, some have called for using that technology to combat terrorism by developing a national identification system. Proponents of such a system argue that a high-tech national identifier system linking Federal and State data bases would allow authorities to spot terrorists before they attack. Some of the September 11th terrorists were in the country illegally. Supporters say had such a system been in place, airline personnel would have been able to cross-check passenger lists against various watchlists. The airlines would have known the men should not have been in the country, let alone on an airplane.

Those who oppose such a system are concerned about the impact a national identifier system would have been on the very precepts of America's freedoms. Given the vast amount of personal information that could be placed in a national identification system, there is legitimate cause for concern over its potential abuse or mismanagement. In the event that such a system were adopted, it must incorporate sufficient safeguards to prevent the abuse of power by those who would have access to the information and those with the authority to demand an individual's identification.

The technical issues involved in a data base project of this magnitude must also be considered. Is it possible to develop a system that is both fraud resistant and secure? Freedom is the most precious gift to Americans. The terrorists knew it and took good advantage of it. Freedom itself was the target of the September 11th attacks. If that freedom is lost in the pursuit of justice, the terrorists will have won even if they themselves are punished. Although holding firm to America's freedoms, we must also be open to new ideas. The survival of this great Nation may depend on it.

[The prepared statement of Hon. Stephen Horn follows:]

DAN BURTON, INDIANA,
CHAIRMAN

BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
JOHN L. MICA, FLORIDA
THOMAS M. DAVIS, VIRGINIA
MARK E. SOUDER, INDIANA
JOE SCARBOROUGH, FLORIDA
STEVEN C. LaTOURETTE, OHIO
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
DAVE WELDON, FLORIDA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
C.L. "BUTCH" OTTER, IDAHO
EDWARD L. SCHROCK, VIRGINIA

ONE HUNDRED SEVENTH CONGRESS

Congreſs of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

FACSIMILE	(202) 225-3974
MAJORITY	(202) 225–5074
MINORITY	(202) 225–5051
TTY	(202) 225–6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
JANICE D. SCHAKOWSKY, ILLINOIS
WM. LACY CLAY, MISSOURI

BERNARD SANDERS, VERMONT,
INDEPENDENT

Opening Statement
Chairman Stephen Horn
Subcommittee on Government Efficiency,
Financial Management and Intergovernmental Relations

A quorum being present, this hearing of the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations will come to order.

Only two months after the devastating terrorist attacks of September 11, this nation is just beginning to understand the dimensions of a dramatically changed world. Preserving the American way of life requires adaptation and sacrifice. It means using this nation's unique strengths to address the vulnerabilities that terrorists exploited at an enormous human toll.

Technology is one of America's greatest strengths. In recent weeks, some have called for using that technology to combat terrorism by developing a national identification system. Proponents of such a system argue that a high-tech, national identifier system linking federal and state databases would allow authorities to spot terrorists before they attack. Some of the September 11 terrorists were in the United States illegally. Supporters say that had such a system been in place, airline personnel would have been able to cross-check passenger lists against various "watch lists." The airlines would have known that the men should not have been in the country, let alone on an airplane.

Those who oppose such a system are concerned about the impact a national identifier system would have on the very precepts of America's freedoms. Given the vast amount of personal information that could be placed in a national identification system, there is legitimate cause for concern over its potential abuse or mismanagement. In the event that such a system were adopted, it must incorporate sufficient safeguards to prevent the abuse of power by those who would have access to the information and those with the authority to demand an individual's identification. The technical issues involved in a database project of this magnitude must also be considered. Is it possible to develop a system that is both fraud-resistant and secure?

Freedom is the most precious gift to Americans. The terrorists knew it and took advantage of it. Freedom itself was the target of the September 11 attacks. If that freedom is lost in the pursuit of justice, the terrorists will have won, even if they themselves are punished. While holding firm to America's freedoms, we must also be open to new ideas. The survival of this great nation may depend on it.

I welcome our witnesses today, and look forward to their testimony.

Mr. HORN. I welcome our witnesses today and I look forward to their testimony, but before giving you the oath, I will yield time for the ranking member, the gentlewoman from Illinois, Ms. Schakowsky, for an opening statement.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman, and I want to thank this panel of witnesses for coming here today. In the wake of September 11th we're faced with an enormous challenge of balancing the need for enhanced national security with a need for protecting civil rights of the public. In the past some efforts in the name of national security, in my view, have gone too far and have endangered those liberties. We've learned that once that kind of harm is done, it's difficult to repair. During World War II, we uprooted thousands of Japanese Americans and placed them in internment camps.

It is generally recognized today over 50 years later that the internment was a mistake. In fact, it was clear at that time there was no danger of sabotage from those individuals.

As historian Margo Anderson points out, in November, 1941, in response to a request by Franklin Roosevelt, John Franklin Carter wrote to the President "There is no Japanese 'problem' on the coast. There will be no armed uprising of Japanese." Nonetheless, thousands of Japanese Americans, many of whom were citizens, were surrounded, rounded up and placed into camps. Today we have a monument to those that were mistreated just north of the Senate office buildings and our government has officially apologized. However getting to that apology and the monument was extremely difficult and did not repair the harm done. The liberty and sense of security lost by those interned cannot be given back. We must be careful not to repeat the mistakes of the past.

Last week on Thursday, before Veterans Day, I went to the floor of the House to pay tribute to those who have served our country in the defense of freedom. We have fought hard throughout our history to maintain a free and open society. We must not sacrifice those freedoms in the name of war. If we sacrifice our freedom, we lose the war no matter what the military outcome. The security measures we propose in response to terrorism must pass three tests. Are they effective? Can they be applied without discrimination? Can they be implemented without sacrificing our fundamental freedoms of due process, privacy, and equality? The proposal for a national identification system is not new. It has failed in the past because it cannot pass these fundamental tests.

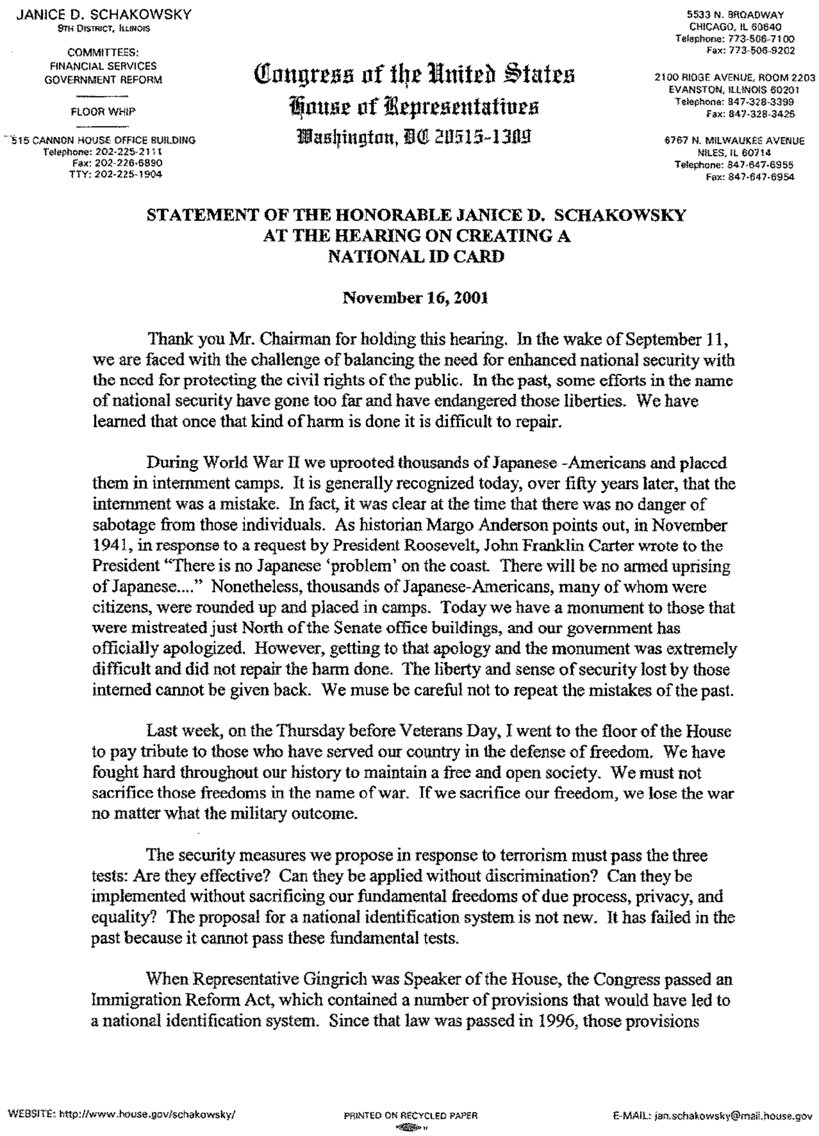
The Congress passed the Immigration Reform Act in 1996 which contained a number of provisions that would have led to a national identification system. Since that law was passed, those provisions have steadily been paved back. One provision was repealed and another modified to the point where it could not be administered at the land border between the United States and its neighbors. In the Patriot Act, the House reaffirmed those provisions knowing that they had no teeth. The events of September 11th show us that systems like national identification cards will not deter crazed terrorists from their mission. Those terrorists all had driver's licenses, credit cards and Internet accounts.

I urge all of us and each of you to pay close attention to the effects your proposal will have on the fundamental freedoms on which this country was founded, freedom of speech and religion, freedom to assembly and freedom of the press, freedom from unreasonable search and seizure and freedom from imprisonment without due process. Those freedoms cannot be ignored in the name of homeland security.

As Members of Congress, we must evaluate any proposal offered in the name of enhanced security. Does it do what it claims to do? What is the burden on the public in terms of time consumed and freedom lost? Do the benefits outweigh the costs, is there an incremental gain in security and does it justify the loss of freedoms?

I look forward to hearing the testimony today and hope our witnesses will help us answer these important questions and I thank you, Mr. Chairman.

[The prepared statement of Hon. Janice D. Schakowsky follows:]



JANICE D. SCHAKOWSKY
9TH DISTRICT, ILLINOIS

COMMITTEES:
FINANCIAL SERVICES
GOVERNMENT REFORM

FLOOR WHIP

515 CANNON HOUSE OFFICE BUILDING
Telephone: 202-225-2111
Fax: 202-226-6890
TTY: 202-225-1904

Congreſs of the United States
Houſe of Repreſentatives
Waſhington, DC 20515-1309

5533 N. BROADWAY
CHICAGO, IL 60640
Telephone: 773-506-7100
Fax: 773-506-9202

2100 RIDGE AVENUE, ROOM 2203
EVANSTON, ILLINOIS 60201
Telephone: 847-328-3399
Fax: 847-328-3425

6767 N. MILWAUKEE AVENUE
NILES, IL 60714
Telephone: 847-647-6955
Fax: 847-647-6954

STATEMENT OF THE HONORABLE JANICE D. SCHAKOWSKY AT THE HEARING ON CREATING A NATIONAL ID CARD

November 16, 2001

Thank you Mr. Chairman for holding this hearing. In the wake of September 11, we are faced with the challenge of balancing the need for enhanced national security with the need for protecting the civil rights of the public. In the past, some efforts in the name of national security have gone too far and have endangered those liberties. We have learned that once that kind of harm is done it is difficult to repair.

During World War II we uprooted thousands of Japanese -Americans and placed them in internment camps. It is generally recognized today, over fifty years later, that the internment was a mistake. In fact, it was clear at the time that there was no danger of sabotage from those individuals. As historian Margo Anderson points out, in November 1941, in response to a request by President Roosevelt, John Franklin Carter wrote to the President "There is no Japanese 'problem' on the coast. There will be no armed uprising of Japanese...." Nonetheless, thousands of Japanese-Americans, many of whom were citizens, were rounded up and placed in camps. Today we have a monument to those that were mistreated just North of the Senate office buildings, and our government has officially apologized. However, getting to that apology and the monument was extremely difficult and did not repair the harm done. The liberty and sense of security lost by those interned cannot be given back. We muse be careful not to repeat the mistakes of the past.

Last week, on the Thursday before Veterans Day, I went to the floor of the House to pay tribute to those who have served our country in the defense of freedom. We have fought hard throughout our history to maintain a free and open society. We must not sacrifice those freedoms in the name of war. If we sacrifice our freedom, we lose the war no matter what the military outcome.

The security measures we propose in response to terrorism must pass the three tests: Are they effective? Can they be applied without discrimination? Can they be implemented without sacrificing our fundamental freedoms of due process, privacy, and equality? The proposal for a national identification system is not new. It has failed in the past because it cannot pass these fundamental tests.

When Representative Gingrich was Speaker of the House, the Congress passed an Immigration Reform Act, which contained a number of provisions that would have led to a national identification system. Since that law was passed in 1996, those provisions have been steadily paired back. One provision was repealed, and another modified to the point where it could not be administered at any land border between the United States and its neighbors. In the Patriot Act, the House reaffirmed those provisions, knowing that they had no teeth.

The events of September 11 show us that systems like national identification cards will not deter the crazed terrorist from his or her mission. Those terrorists all had driver's licenses, credit cards, and Internet accounts.

I urge each of you to pay close attention to the effects your proposal will have on the fundamental freedoms on which this country was founded – freedom of speech and religion, freedom to assembly and freedom of the press, freedom from unreasonable search and seizure, and freedom from imprisonment with out due process. Those freedoms cannot be ignored in the name of homeland security.

As members of Congress we must evaluate any proposal offered in the name of enhanced security. First, does the proposal in fact do what it claims to do? Second, what is the burden on the public in terms of time consumed and freedom lost? Third, do the benefits outweigh the costs -- is there an incremental gain in security and does it justify the loss of freedoms?

I look forward to hearing the testimony today, and hope our witnesses will help us to answer these important questions.

Mr. HORN. I thank you and before I call on Mrs. Maloney, we have two Members of Congress which will be before us, and without objection, we'll have Mr. Castle and Mr. Miller. And Mr. Castle.

Mr. CASTLE. Thank you very much, Mr. Chairman, I know I'm an interloper here today and I appreciate you and the ranking member allowing me to appear. I wanted to share some thoughts I have on this and some legislation I've been working on with Congressman Jeff Flake of Arizona with respect to this issue. But I must comment first, this is a very distinguished, but even more so, a very interesting panel. I look forward to what they have to say.

Many of the issues that are involved in the subject matter of today of national identification cards, in my judgment, should first be addressed in managing foreign visa holders in the United States of America. While I understand that the issue of national ID cards is extremely important in the times we are living in, and I imagine somewhat controversial if I had to place a wager on it, I believe that we must first begin with the tracking of foreign guests in our country, and I don't think this should be controversial.

I would like to share a few statistics with you. In 1998, the Immigration and Naturalization Service [INS], reported that 30.1 million foreign people came to the United States on a temporary basis. Of those 30.1 million, there are an estimated 5 to 8 million illegal immigrants living in the United States, 40 percent of which were listed as overstays by the INS. That means they stayed beyond the time of their visa. I believe very strongly, and Mr. Flake does as well, that we need to be able to monitor all foreign visitors and track in real-time, that is, the actual knowledge on a computer screen in real time who they are, what their background is, and what they are doing in our country.

Congress is actually—probably in the time of the gentlemen that are on this panel—has actually, taken steps on this, but none of this has really been implemented. Six years ago the Congress directed the INS to gather the arrival and departure date of most foreign visitors to make sure they do not remain in the United States after the expiration of their authorized stays, however, to this day the INS passenger accelerated service system, INSPASS is its acronym, remains only a pilot project used in only four airports, but not in any land or seaport points of entries.

Another example of an innovative idea which has been put in place but not fully used, is a border crossing card which is used by Mexican and Canadian nationals who seek admission as border crossers, but again, this program has been plagued by difficulties and delays. I think such examples illustrate the lost opportunities inherent in the poor management of tracking systems. To address immigration challenges, Representative Flake, Representative Deal of Georgia and I did introduce an act called the ISA, Integrity and Security Act, to strengthen the immigration system and to improve the ability of the INS to track all these temporary visa holders.

A number of the key provisions in this legislation were actually included in the Patriot Act, which you might know as the Antiterrorism Act, which passed very recently in the Congress of the United States.

But there is still a lot of work to be done. We do need to be able to track and locate temporary foreign visitors to the United States to ensure they are here for their stated purpose, which could be anything from being a student to working, to a visitor, and to know when they have come and when they have left. A student tracking system that has been under development since 1997 needs to be improved and fully implemented. The Patriot Act does call for the implementation of the student tracking system and it's authorized $36 million, which is a good start toward its deployment. However, we must advocate that the INS incorporate key provisions in any future student tracking system. We need to know if foreign students actually enroll in classes and whether they drop out.

There are over 500,000 foreign students in the United States now. We also need to know their family history, course of study, and date of enrollment. And second, we need to know if a temporary worker holding an H1B visa, which has been the subject matter of many an hour here in the Congress, is still working at the company that hired that person. A crucial aspect of any effective system that tracks foreign visitors is the use of technology to foil would-be counterfeiters; of which there are many, I might add.

A smart card visa for foreign visitors would be much more difficult to forge than traditional visas. It would hold a copy of the fingerprint biometric and typical visa information, or a pupil of the eye or whatever biometric one would want to use. This is not a new idea either, by the way. It just has not been implemented particularly well. U.S. citizens across the border frequently are able to participate in a voluntary program that registers a fingerprint biometric. We just think in certain instances it should be automatic that it be done as opposed to being a voluntary program. The holders of frequent travelers passports pass more quickly through Customs by showing their fingers for identification at a Customs station.

The use of biometric technology is encouraged in the Patriot Act. These tamper-resistant bases could eventually be linked to an integrated computerized entry/exit system and the INS, Customs, consulates, universities and other law enforcement agencies would all work off the same information to monitor and track students, tourists and other visa holders. I'm sure I'm not telling anybody here the difficulty of some of the information exchange, even among governmental agencies today, much less sort of computer in real time in terms of the various places, the Embassies, the points of entry where that information would be useable. All this technology is available, by the way, although at a cost, and programs could be more effectively utilized to track our foreign guests.

The lessons learned from tracking foreign visitors can lend important insight to the pros and cons of enacting a national identification card for U.S. citizens, which we may or may not be ready for now, but I think we are ready for a visa system at this point if we put our minds to it and go about it.

Let me just say in conclusion, in no way am I advocating limiting, in this particular program, what we are doing with respect to visas or visitors to our country. We just want to make sure we know who's coming into this country, and if they should not be coming into this country, preventing them from being here and while they are here, they are doing what they are supposed to be doing.

I appreciate the time, Mr. Chairman. Again, I realize I'm an interloper, and you have been very generous and I yield back to the balance of my time.

Mr. HORN. Thank you very much.

[The prepared statement of Hon. Michael N. Castle follows:]

JOINT STATEMENT OF
THE HONORABLE MICHAEL N. CASTLE AND THE HONORABLE JEFF FLAKE

GOVERNMENT REFORM SUBCOMMITTEE ON GOVERNMENT EFFICIENCY
FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS
"OVERSIGHT HEARING ON NATIONAL IDENTIFICATION CARDS"

NOVEMBER 16, 2001

I want to thank the Chairman and Ranking Member for indulging my presence at the Subcommittee today. This is such an important issue to our nation that I requested this opportunity to read a joint statement Congressman Jeff Flake and I have drafted. While it is important to begin the far-reaching debate on identification cards for citizens of this country, we should first address the issue of the inadequate system for identifying and monitoring foreign visitors to the U.S.

Many of the issues that are involved in the question of national identification cards should be first addressed in managing foreign visa holders in the United States. Millions of these visitors overstay their visas, and we need a much better system and documents for enforcing the terms by which they enter and leave our country. An estimated 40 percent of the five to eight million illegal immigrants living in the United States last year were listed as overstays by the INS, although the agency admits that 1991 is the last year for which it can estimate the number of visa over stayers with any accuracy.

It is imperative that we make immediate changes in our ability to document and track foreign visitors to the U.S. to thwart future potential terrorist acts. This will require improved documentation and computerized systems for tracking the millions of foreign visitors who come to our nation each year on a temporary basis with tourist, student, or temporary work visas. In 1998, the Immigration and Naturalization Service (INS) reported that 30.1 million foreign people came to the United States on a temporary basis.

A fresh look at the execution of the visa processing program is, without a doubt, necessary. Six years ago, Congress directed the INS to gather the arrival and departure data of most foreign visitors to make sure they do not remain in the United States after the expiration of their authorized stays. A recent review by the Department of Justice Inspector General found that INS officials mismanaged $31 million aimed at automating that system.

Efforts to implement such an "entry-exit program" have moved at a snail's pace. Congress first gave INS a directive to implement an automated entry-exit tracking system for land borders and seaports in 1996 as part of the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA). However, to this day, the INS Passenger Accelerated Service System (INSPASS) *remains only a pilot project*. This pilot system is used at airports in Philadelphia, Pittsburgh, Charlotte and St. Louis, and only two airlines are participating. It is not used at any land or seaports.

Another program that has enormous potential for tracking those who enter our country, while at the same time facilitating their passage, is the Border Crossing Card used by Mexican and Canadian nationals who seek admission as daily border crossers. However, even this program has been plagued by difficulties and delays. INS has failed to implement the requirements of section 104 of the IIRIRA that mandated the implementation of a system to provide new machine-readable biometric Border Crossing Cards. After recognizing the potential for fraud inherent in the cards, which permit residents of Mexico to cross the U.S. border and travel up to 25 miles within the United States, Congress mandated the creation of new border crossing cards containing a machine-readable biometric identifier. Although INS has issued cards, it has failed to select or procure the scanning equipment for those cards, and failed to begin work on the system to process information on the aliens to whom the cards were issued.

Thus, the four million cards that have already been issued cannot be read by machine, nor is there a system in place to process the information relating to the card holders. The cards continue to be issued at a rate of 50,000 per week, but INS has failed to utilize efficiently information technology which would permit quick and secure processing of border crossers.

Such examples illustrate the lost opportunities inherent in the poor management of tracking systems. As we have learned, the Federal Government has no record of how 6 of the 19 September 11 hijackers entered the United States. An additional 4 of those terrorists were visa over stayers. As we seek to improve our national security, reform of the visa processing system should be among our highest priorities.

One of the terrorists on the plane that crashed into the Pentagon could have been stopped if we monitored student visas. Saudi national Hani Hanjour was supposed to attend an English Language School in California and never showed up for school. The man who was just caught attempting to smuggle knives and a stun gun on a flight in Chicago is in the United States on an expired student visa. In 1993, Eyad Ismoil, one of the terrorists who drove a truck bomb into the World Trade Center, was here on an expired student visa.

Representative Flake, Representative Nathan Deal and I recently introduced legislation, **H.R. 3077, The Visa Integrity and Security Act (VISA Act),** to strengthen our immigration system and to improve the ability of the INS to track all temporary visa holders. A number of the key provisions in this legislation were included in the Patriot Act.

However, there is much more work to be done. We need to be able to track and locate temporary foreign visitors to the U.S. to ensure they are here for their stated purpose and only stay for the allotted time.

A student visa tracking system that has been under development since 1997 needs to be improved and fully implemented. The Patriot Act calls for the full implementation of the student tracking system and has authorized over $36 million towards its deployment. However we must advocate that the INS incorporate key provisions in any future student tracking system. We need to know if foreign students actually enroll in classes and whether they drop out. There are over 500,000 foreign students studying in the United States. We need a means to locate them if they stop their studies and try to remain in the United States. We also need a secure and immediate method to identify students and other foreign guests. Furthermore, we need to know if a temporary worker holding an H-1B visa is still working at the company that hired that person. We have proposed in our legislation that a company sponsoring a holder of an H-1B visa report to the Attorney General the termination date and reasons no later than 14 days after the termination.

A crucial aspect of any effective system that tracks foreign visitors is the use of technology to foil would-be counterfeiters. A "smart card" visa for foreign visitors would be much more difficult to forge than traditional visas. It would hold a copy of the fingerprint biometric and typical visa information. The holder would be required to present his or her finger to have it matched to the copy on the chip to prove their identity. As yet, the INS has failed to deliver such a program.

Using biometrics to manage border crossings is not a new idea in the United States. U.S. citizens who cross the border frequently are able to participate in a voluntary program that registers a fingerprint biometric. Holders of frequent-traveler passports pass more quickly through customs by showing their fingers for identification at a customs station. The use of bio-metric technology was encouraged in the Patriot Act. These tamper resistant visas could eventually be linked to an integrated, computerized entry-exit system and the INS, Customs, Consulates, Universities and other law enforcement agencies would all work off the same information to monitor and track students, tourists and other visa-holders.

The technology is available and programs can be more effectively utilized to track our foreign guests. Now is the time to work together to make sure that every initiative is implemented to improve the security of our country. We can still welcome foreign visitors, but we have the right and duty to know they are in our nation for the right reasons and set the terms for their stay. The lessons learned from tracking foreign visitors can lend important insight to the pros and cons of enacting a national identification card for U.S. citizens.

Mr. HORN. And now I yield to the ranking member over the years and the gentlelady of New York, Mrs. Maloney.

Mrs. MALONEY. Thank you. And I would first like to thank you, Mr. Chairman, and the ranking member, for tackling yet another complicated and controversial issue. Also I'd like to extend my appreciation to the very interesting panelists you have assembled here today for taking the time to be here. We have taken a hard look at the way our great Nation operates since September 11th.

The hard cold truth is that we have been very lax in many years of safety and security. I believe the most difficult fact for us as a Nation to face is that there is a group of individuals who hate us and want to do harm to the citizens of America. As an elected official, I must do everything that I can to protect my constituents and the constituents of our country. In this new world, I am not exactly how sure we can accomplish this; however, I am eager to learn and understand more as we will today.

In the month of October alone, we had 17 million people travel across the borders of the United States. We welcome all travelers. Our Nation's economy depends in part on these visitors. However, we have to face the cold hard truth that not everyone entering our borders enters with good intentions. Access to the United States must be looked upon as a privilege, not a right. Our country's founders provided many safeguards to protect our freedom while ensuring our safety. One of the beauties of our democracy is that it is not static, but a robust living thing that can change, and times have dramatically changed.

Daniel Webster, one our Nation's former great leaders once stated, "God grants liberty only to those who love it and are always ready to guard and to defend." Today we must guard and defend it. We must not be afraid of new ideas. We need to protect not only the rights of individuals but their life. We pride ourselves in the many freedoms we have in the United States. However, in order to protect these freedoms we need to protect our safety and our Nation's security. I commend President Bush for taking the bold step yesterday to begin to require stricter regulations regarding the granting of visas. Fear has struck the core of the community I represent in New York. I lost well over 600 constituents, and it has struck the core of the American people.

The freedom to travel freely about our Nation has taken a devastating blow. We now have armed guards on several flights with implementation of complete coverage for all flights ongoing. We look to our law enforcement to protect and to serve; however, we need to arm them with the tools to accomplish this mission. A more thorough and smarter green card for non-U.S. persons, I believe, is a beginning.

I also believe that we need to tie one's State driver's license to their visa expiration date. During a hearing held in New York on terrorism, Governor Jeb Bush provided testimony that in his State of Florida, one's driver's license expires the same date as their visa. Does this not provide yet another way of tracking non-U.S. persons?

I believe we need to take other steps, and one could be that an individual's bank account could be frozen also at the time of a visa expiration date. All non-reclaimed funds could revert to the State's escrow account to fight terrorism. We have seen how our banking industry has been contaminated by the terrorist community again and we need to reclaim it. As I have stated earlier, I do not have all the answers; so I'm very much looking forward to our panelists to help me and other members of this committee uncover all the pros and cons of this important issue. Thank you very much and I yield back Mr. Chairman.

Mr. HORN. Thank you.

[The prepared statement of Hon. Carolyn B. Maloney follows:]

14th District • New York

Congresswoman

Carolyn **Maloney**

Reports

2430 Rayburn Building • Washington, DC 20515 • 202-225-7944
1651 Third Avenue • Suite 311 • New York, NY 10128 • 212-860-0606

PREPARED STATEMENT OF

CONGRESSWOMAN CAROLYN B. MALONEY

before the Government Efficiency, Financial Management,
and Intergovernmental Relations Subcommittee
of the Government Reform and Oversight Committee

November 16, 2001

I first would like to thank the Chairman for holding this hearing and commend him for tackling yet another complicated and controversial issue. Also, I would like to extend my appreciation to the panelists for taking the time to attend today's hearing.

We have taken a hard look at the way our great nation operates since September 11th. The hard, cold truth is that we have been very lax in many areas of safety and security. I believe, the most difficult fact for us as a nation to face is that there is a group of individuals who hate us and want to do harm to the citizens of America. As an elected official I must do everything that I can to protect my constituents and the constituents of our country.

In this new world, I am not exactly sure how we can accomplish this however, I am eager to learn and understand the issues.

In the month of October alone, we had 17 million people travel across the borders of the United States. We welcome all travelers. Our nation's economy depends in part, on these visitors. However, we have to face the cold, hard truth that not everyone entering our borders enters with good intentions.

Access to the United States must be looked upon as a privilege not a right. Our country's founders provided many safeguards to protect our freedom, while ensuring our safety. One of the beauties of our democracy is that it is not static, but a robust, living thing which can change; and times have dramatically changed. Daniel Webster, one of our nation's great orator's, stated: "God grants liberty only to those who love it, and are always ready to guard and defend it." Today we must guard and defend it. We must not be afraid of new ideas. We need to protect not only the rights of individuals but their life. We pride ourselves in the many freedoms we have in the United States. However, in order to protect those freedoms we need to protect our safety and nation's security. I commend President Bush for taking the bold step yesterday to begin to require stricter regulations regarding the granting of visas.

Fear has struck the core of the American people. The freedom to travel freely about our nation has taken a devastating blow. We now have armed guards on several flights with the implementation of complete coverage for all flights ongoing.

We look to our law enforcement to protect and to serve. However, we need to arm them with the tools to accomplish this mission. A national identification card for non-U.S. persons I believe is a beginning. I also believe that we need to tie one's state drivers license to their visa expiration date. During a hearing held in New York by the Permanent Select Committee on Intelligence, Subcommittee on Terrorism and Homeland Security, Governor Jed Bush provided testimony that in his state, of Florida, one's driver's license expires the same date as their visa. Does this not provide yet another way of tracking non U.S. persons? I believe we need to take this idea one step further wherein an individual's bank accounts are frozen also on the expiration date. All non-reclaimed funds revert to the State's escrow account. We have seen how our banking industry has been contaminated by the terrorist community, again we need to reclaim it.

As I stated earlier, I do not have all the answers so I am looking to you, our panelists, to help me and the members of this subcommittee uncover all the pros and cons of the issue.

Thank You.

##

Mr. HORN. And we now yield to Mr. Miller from Florida, the chairman of the Census Subcommittee of Government Reform.

Mr. Miller.

Mr. MILLER. Thank you, Mr. Chairman. Thank you for calling this hearing. I'm delighted with the two panels and I will be very brief because I heard the Speaker talk about this briefly at a breakfast about 2 weeks ago, and ever since, September 11th has raised a lot of issues as to the direction this is going to go—civil liberties issues, and I know this will be addressed by the panel, the privacy issue, which Mr. McCollum has worked on a lot, technology, which the Speaker has talked about all the time, and just to make sure our country can function after post-September 11th, our economy. So there's a lot of challenges and interesting comments and I'm really here to listen and learn. So I yield back.

Mr. HORN. Thank you very much.

And any other statements that come in will be filed for the record. We now start with our first panel, and I think you know the routine, that this is an investigating committee, and so if you raise your right hands and if you have any assistants backing you up, get them and the clerk will get their names too.

[Witnesses sworn.]

Mr. HORN. The clerk will note that all the witnesses have affirmed, and we start with the Honorable Newt Gingrich, former Speaker of the U.S. House of Representatives.

Mr. Speaker.

STATEMENTS OF HON. NEWT GINGRICH, FORMER SPEAKER OF THE U.S. HOUSE OF REPRESENTATIVES; HON. ALAN SIMPSON, FORMER MAJORITY WHIP OF THE U.S. SENATE; AND HON. BILL McCOLLUM, FORMER CHAIRMAN, PERMANENT SELECT COMMITTEE ON INTELLIGENCE, SUBCOMMITTEE ON HUMAN INTELLIGENCE, ANALYSIS AND COUNTERINTELLIGENCE, FORMER CHAIRMAN, JUDICIARY'S SUBCOMMITTEE ON CRIME, U.S. HOUSE OF REPRESENTATIVES

Mr. GINGRICH. Thank you very much, Mr. Chairman, and I want to thank you and the ranking member for holding this hearing. I also want to take this opportunity to commend you for your consistent leadership on the issue of cybersecurity and the fact that this subcommittee has been very far ahead of events in looking at the need for effective technology in the security area. I also want to begin with Mrs. Schakowsky's, I think, absolutely correct point, which is that we have to design—the challenge to the Congress and the President is to design—the system which both provides civil liberties protection for the innocent and protection of the innocent.

In the past, with things like fingerprinting, wiretapping and other technologies, we've worked very hard to make sure that while we were strengthening law enforcement we were never infringing on the innocent, and I think this has to be thought through in a very careful way. The fact is, we already have a primitive inefficient, easily cheated system of identification. I flew out of Reagan National yesterday, and three times I produced an ID card.

Now, I just want to point out every audience I've talked to around the country, I've asked them how many of them know someone who in high school had an access to an ID card that might not have been their own for reasons we won't go into. And while no one personally had ever used an ID card for an inappropriate purpose, it always amazed me the number of people who seem to find, at 16 or 17, access to an ID card.

So I want to be very clear. I think we have already indicated at airports, we've indicated at government buildings, we've indicated in a variety of places that asking for identification is legitimate. The question now is can we design a system which has an effective ID style while protecting the innocent? I think that it has to be an American model of security, which means a high technology capital intensive system that provides security, speed, efficiency, and convenience.

That's the model we've always set for ourselves, and I think, frankly, the current lines at airports are a sign we don't have a system that meets that test. It's necessary for the world economy to have a parallel system for freight, whether it's in trucks or container cargo that is secure, fast, and efficient, or we will literally break down the world economy and add a substantial amount of cost to everybody's life.

I would suggest to this subcommittee that as you look at these, that you look very seriously at outsourcing as much production as possible because most of the great breakthroughs that are high technology and capital intensive occur in the private sector and occur in entrepreneurial businesses. I particularly would recommend Clayton Christiansen's, the Innovator's Dilemma, as a study of new technologies that work, and Nathan Merival's recent writing, particularly in USA Today, on the concept of exponential industries and the ability to develop really dramatic new technologies in the next 5 to 10 years.

I personally think we are going to want to end up with a biometric solution that involves either a retinal or iris scan, which I think is harder to cheat than the thumbprint, and frankly, is as easy to measure in real time. It's simply a picture, and any of us who are being filmed for television or still photographers are having exactly the same experience you'd have for a retinal scan.

I want to distinguish also civil liberties for American citizens from foreign visitors. I believe that all foreign visitors should be scanned as they enter the country. We ought to have a data bank either of their iris or retina. I think that's the technical decision of which one you're using. But we ought to be able to know who you are. We ought to be able to match you up against a system that would indicate whether you were a known drug dealer, a known terrorist, etc., and that would basically indicate and attach to an identity that had a biometric on the identity card, so we knew that the person we're talking to didn't just buy this for $11 in Los Angeles on a street corner as can currently be done.

For Americans, I think it's fairly simple to have the 50 States go to a biometric measure on the driver's license and simply ensure that all of the States—50 States plus D.C. have their data bases linked. That means an investment in wireless high-speed connectivity with very high-speed computing, but literally it's no harder for a policeman standing and talking to you beside your car within seconds to verify who you really are, if we design a system that does it, and I think you can do that with civil liberties protected.

I would not insist on a national ID card because I think you do get into civil libertarian issues, but I would suggest to you that the simple act of having two lines in airports, one biometric where anybody who's a frequent flyer who wanted to be able to literally walk through the line, verify who they are, and pickup their ticket at security as they're going through, while we'd have a long line that may take an hour and a half for people who prefer to avoid that kind of convenience.

I think you'd find a natural migration of over 90 percent of the American travelers within a year or less to the higher speed line. Let me also suggest that the committee look at the emerging technology at MIT and elsewhere, that for somewhere between 1 and 30 cents per suitcase you could literally have an embedded wireless system that would enable you to track literally every suitcase, and if you introduced it as a manufacturing process now, you would, within 5 or 6 years, have an overwhelmingly tagged and identified highly secure system.

As I said earlier, this kind of thinking, I think, has to also apply to trucks and to container cargos. And if you look at what UPS and FedEx already do, you can see the beginnings of a model that given the high—the new breakthroughs and the new technologies can be even more sophisticated and even more accurate. Let me just close by going back to the exactly correct warning that Mrs. Schakowsky made. There is no question in my mind that we can design, just as with medical records, an ability to have personal privacy and access to information that may save our lives, but that probably requires a Federal law that makes it a felony to use that medical record inappropriately.

Similarly I think you can design a system which allows you to track a person who is generally out to do something bad without, in that process, either dramatically inconveniencing or harming those who are innocent, and in fact, I would argue that if the American people knew that every employee who walked on an airport had some means of checking to make sure they were really the person they claimed to be, if we knew that our FBI, CIA, FAA computers worked, the notion—I just want to close on this notion, because what you're doing on this subcommittee is so vital.

Six weeks before September 11th, the Central Intelligence Agency told the Federal Bureau of Investigation two terrorists had entered the United States. Six weeks later, they had still not be able to get that information into the airline computers, and two of the terrorists on September 11th in Boston boarded the airplane under their own names, 42 days after the U.S. Government officially knew they were in the United States and they were very dangerous.

Now, I simply suggest going to a mandatory regular ID card won't help much because with desktop printing they will learn how to buy cards that are false, but if we had a high-speed computing system and we had an ability to have very high speed access, I think we could design a system where we would have found those two people, they would have been stopped at Logan, and we would have had a very significant understanding of what was going on.

I think this committee's moving in the right direction. If it does it right, the system will be very secure, it will be very safe and it will protect our civil liberties while also protecting us.

Mr. HORN. We thank you very much for those pertinent views which I'm used to and it's very useful. We now turn to the very distinguished ex-Senator and one of the great public servants of this country, namely Alan Simpson, who spent more time on immigration I think than probably all the rest of us put together. So I'm going to turn it over to you——

Ms. SCHAKOWSKY. Mr. Chairman, if I could just inquire, apparently you're going to proceed through the vote?

Mr. HORN. No. We're going to go now and when Mr. Miller returns, he will be presiding and then I will come back. We're in this less-than-seamless operation known as the vote.

Mr. SIMPSON. We know that.

Mr. HORN. And we'll be back——

Mr. SIMPSON. I will just proceed, then. Thank you.

Mr. HORN. Proceed, and then I will try to be back in 6 or 7 minutes.

Mr. SIMPSON. Thank you, Chairman Horn. I come in here with a very eerie feeling as Jack Brooks is staring at me there. He would look at me with that smouldering cigar and say Simpson, I've got a deal for you. God, I'd lose my shirt and my underwear and everything else in here. Well, that was Jack Brooks. What an amazing man.

It is a pleasure to be here to discuss this serious issue of how we might strengthen domestic security. I was particularly moved by Congresswoman Schakowsky's remarks where I met Norm Mineta at the Hart Mountain Relocation Center when we were 12-year-old boys. He was behind wire and I lived in Cody, and our scoutmaster took us to the Jap camp, is what it was called, 11,000 people there.

And Norm and I struck up a friendship of curiosity and juvenile development that has lasted 70 years. He is a very dear and special friend, but we'll want to remember at that time, Attorney General Warren, Earl Warren of California, signed the order to evacuate them, and the unanimous decision of the U.S. Supreme Court by William O. Douglas said that it was proper. So I think let's keep that into perspective and not think of how it is 50 years from then as to the fact that the Japanese submarine lobbed a couple of shells into an oil field off of California in the Spring of 1942, and it kind of startled people. Just thought I'd pitch that in. Just thought I'd throw it in there.

Anyway, you're on track. I was impressed by what Newt is saying because you're all being led astray by a single term, and the term is national ID. I never used it. I put it in the bill that we are now talking about a national ID, and you do a disservice to the country when you use the phrase national ID. We're talking about a more secure identifier system. It could be many things, and if anyone believes there is intrusiveness in what we are suggesting, all of us, Newt, myself, what Bill will say, what Democrats and Republicans—what Rodino and I said, what Mazzoli and I said.

And in the bill, it said we're not talking about a national ID. That's a diversion for people who like to talk about tattoos and

Nazi Germany and don't let them get away with it. We're not talking about that. Every time we tried to do something in this area, it was filled with emotion, fear, guilt, and racism. The Select Commission on Immigration and Refugee Policy said we ought to do something in this area. We tried to do that, got shot out of the saddle by arguments about tattoos and Nazi Germany. Then we tried it again and we had a biometric activity in one of them, and in a conference committee in the middle of the night when on the floor of the House passed, the Senate, there was an emotional, highly emotional argument about, again, Nazi Germany and tattoos. It was pulled out and dear old Joe Moakley took it out and we passed it in the middle of the night without anything in it.

The House always had an aversion to that kind of thing. The Senate would pass it. And I can only share with you that everything we did in this area was bipartisan. Mazzoli, Democrat from Kentucky, Rodino, the chairman of the Judiciary Committee from New Jersey, still living, and a magnificent man, we did these things—Hamfish, and Newt knows him well and so did Bill. You have to do something, and the something is not intrusive any more than what you get when you go to the airport now or what you get when you go into a store and have to give your slide card or when you file for credit or whatever it may be——

Ms. SCHAKOWSKY. Senator Simpson.

Mr. SIMPSON. Yes, indeed.

Ms. SCHAKOWSKY. I'm afraid I have to go vote, which would leave no Members here. And so I'm going to grab this gavel while I can and recess this committee at least until someone returns. All right?

Mr. SIMPSON. Well, that's very kind. Thank you. I'll just keep going though. No.

[Recess.]

Mr. MILLER [presiding]. The subcommittee will come back to order. Mr. Horn will be back shortly and asked me to proceed with the presentation. I think, Senator Simpson, would you continue?

Mr. SIMPSON. Thank you, Congressman Miller, and I see you have new devices which are very clearly, which aren't on yet, so I will speed ahead—I was just kind of reviewing things and speaking to Congresswoman Schakowsky's comments. Let me just give us a very brief summary of past efforts. The Select Commission came into being 1979 to 1981. I was a member of that bipartisan commission. Father Ted Hesburg was chairman, and we did a lot of things. We recognized that no system attempting to control anything would be effective without a more secure method of confirming a person's identity and immigration status.

So we recommended, the Commission recommended—it was a narrow vote, substantial improvement. Then we had the Immigration Reform and Control Act of 1986. When that first passed, it had a provision in it that the executive branch would implement a system that would reliably determine identity again and authorization of all persons. That was weakened by the Senate and stripped by the House. I think it was a conference committee and that's often the history of conference committees as I recall them here in this Chamber, especially with Brooks with the gavel.

But anyway, that's an aside. The enacted version of IRCA had a pilot program in it, and then we had telephone verification. We couldn't get much done because, again, the background noise was always national ID. The initial conference committee version of the Immigration Act of 1990 where we broadened legal immigration a great deal, contained a pilot program using biometric data to make State driver's licenses more secure, and it was then to the amazement of Democrats and Republicans alike that issue demagogued in the most grotesque way one evening in this House body, and the House rule was defeated and Joe Moakley brought it back from the dead, and we got it out but it was stripped again.

Then Barbara Jordan came to the fore, the most amazing woman, and she did the Jordan Immigration—Commission on Immigration Reform. She recognized it was too susceptible, the present system was too susceptible to discrimination against foreign-looking or foreign-born or foreign-sounding workers; so she commended a computerized registry using data provided by Social Security and the INS and suggested pilot programs for employers to use these data bases to be conducted in States with the highest immigration rates.

Then along came the 1996 bill. I had little to do with that because we did nothing to do anything to curb illegal immigration—or legal immigration, rather, as Barbara Jordan recommended, but we did get a pilot program in there to—where you could access by computer modem. In 1997, it was used by approximately 2,000 employers who were voluntarily using it. While it's a helpful deterrent to certain instances of fraud, it is not a good one. An unauthorized alien submits a card with an invalid number or submits a card where the name does not match a number, it does not prevent aliens who falsely assume the identity of another person from using the other person's valid Social Security number, and this is often referred to as identity theft or true identity fraud and it is endemic in America.

Talk to your credit card people. So I doubt that there is any full support for a national ID card. I never suggested it and I just have to pack that in one more time. And if that's going to be the word, you're going to all fail. You will do nothing. Get away from it. It's a phony baloney. What we're talking about is—and when we were talking about it then—some type of new document to establish work authorization or identity. We were talking about perhaps a card that would not be carried on your person, not be used for law enforcement, have the maiden name of your mother on the back of it, and the birth date. And then you know always would come the George Orwellian aspects of that.

Here's what I suggest respectfully. A few positive benefits, I think. I therefore would respectfully suggest that you improve the safe—the State driver's licenses. That's the principal identity document in our country. We must eliminate the ability of people to falsely assume the identity of another. Some of the September 11th terrorists facilitated their actions through easy access to Virginia driver's licenses. Now, the only way to prevent identity fraud is to improve biometric data on the card. I agree with Newt completely, such as a fingerprint. It is also—in California, it is done with a retina scan in California for commercial driver's licenses. You'll want to take a look at that.

Minimum nationwide issuance standards could be imposed by the Congress or agreed upon by the States. I think it would be minimally intrusive. Expanded access would be another one to INS and Social Security data bases, extend the basic pilot program, not just California, New York, Texas, Florida or Illinois. Include other States; have access to that base. Of course, that would require more funding for the Social Security Administration and directing to improve the accuracy of the data base. And here's the one that everybody misses, there are about 2,000 agencies of the United States that issue a birth certificate. They love it. They're little old ladies. They do things, little old men, and they issue them and they love it. They don't want anybody to mess with me giving—because I know the mother and the father and when little twinkle toes was born, I signed that.

The vulnerability of the birth certificate system allows aliens to bypass all immigration systems altogether and impersonate U.S. citizens. The Jordan Commission said if we reduce the fraudulent access to the breeder documents, start looking at the breeder documents, ladies and gentlemen of the Congress, particularly birth certificates that can be used to establish an identity of this country and the specific steps recommended by her commission were, and I conclude, regulation of requests for birth certificates through standardized application forms, a system of interstate and intrastate matching of birth and death.

We don't do that in America. We don't match birth and death. How can you ever get a handle on it? Requiring a Federal agency only accept certified copies of birth certificates and a standard design and paper stock for all certified copies and encouraging the States to computerize birth records repositories. I think these recommendations are sensible, practical, and should be enacted and it is time. Thank you very much.

Mr. HORN [presiding]. Thank you, Senator. As usual you have the common people's touch and you also know how to get through the bureaucracy and everything else. I am glad to say to you the commissioner yesterday told a number of us that he will split up the agency so that you've got an enforcement operation and you've got a service operation and a lot of us have wanted that over the years. So a little progress is being made there.

[The prepared statement of Hon. Alan Simpson follows:]

Statement of Alan K. Simpson

Subcommittee on Government Efficiency

House Committee on Government Reform

November 16, 2001

Mr. Chairman and members of the subcommittee, I thank you for this opportunity to discuss how the United States might strengthen its domestic security by improving the security of its identity and work authorization documents.

As you may know, I spent a good portion of my Senate career working to reform our nation's immigration laws. No problem was ever more apparent than the susceptibility of federal, state and local documents to fraud and misuse. And no problem was ever politically more difficult than trying to pass legislation to improve these documents. The issue is filled with emotion, fear, guilt and racism. The horrific events of September 11, 2001, however, compel Congress to reconsider these tough issues.

History. Improving the security of identity and work authorization documents has been under review by policy-makers since at least the late 1970's, and was last addressed by Congress in the 1996 immigration act. I feel that a brief summary of these past efforts may be helpful to those who are considering new reforms today:

Select Commission on Immigration and Refugee Policy. From 1979-1981, I was member of this bipartisan commission, chaired by Father Theodore Hesburg. The SCIRP recognized that no system attempting to control the unauthorized presence or employment of aliens would be effective without a more secure method to confirm a person's identity and immigration status. By a narrow margin, the Commission recommended substantial improvements to the social security card.

Immigration Reform and Control Act of 1986. When this legislation first passed the Senate in 1982, it contained a requirement that the Executive Branch implement a system that could reliably determine the identity and work authorization of all persons applying for new employment in the United States. Subsequent versions of the legislation were weakened by the Senate, and the House voted to strip any improvements in current documents whatsoever. The House's political aversion to making documents more secure prevailed in conference. The enacted version of IRCA provided pilot programs for "telephone verification" but resulted in no substantive improvements in current documents.

Immigration Act of 1990. The initial conference-committee version of this law contained a pilot program studying the use of biometric data to make state drivers' licenses more secure. To the amazement of many Democrats and Republicans from the House and Senate alike, opponents of the legislation demagogued the issue of "biometric identifiers" – with references to "tattoos" and "Nazi Germany" -- and defeated the House rule for consideration of the conference report because of this provision. The provision was subsequently deleted and the legislation was enacted without any reference whatsoever to improvements in state drivers' licenses.

Jordan Immigration Commission. In 1994, the U.S. Commission on Immigration Reform recognized that the current worker verification system was too susceptible to fraud and also believed it could lead to inadvertent discrimination against "foreign-looking" or "foreign-sounding" workers. It recommended a computerized registry using data provided by the Social Security Administration and the INS, and suggested that pilot programs for employers to use these databases be conducted in states with high immigration rates.

Illegal Immigration Reform and Immigrant Responsibility Act of 1996. The 1996 act incorporated the Jordan Commission's "pilot program" recommendation, directing INS to create a computerized database that participating employers could access by computer modem in order to determine the validity of social security numbers and INS numbers. This program, known as the "Basic Pilot," began operations in 1997 and has approximately 2,000 employers voluntarily using it today. While it is a helpful deterrent to certain levels of social-security-card fraud (for instance, when unauthorized aliens submit a card with an invalid number, or submit a card where the name does not match the number), it does not prevent aliens who falsely assume the identity of another person from using the other person's valid social security number. This is often referred to as "identity theft" or "true identity fraud."

Reform Proposals. I do not believe there presently is full political support -- or the practical need -- for a new document to establish the identity and work authorization of every person authorized to be in our country (emotionally labeled a "National I.D. Card"). Improvements in a few current documents, however, would greatly increase our domestic security and would have positive immigration benefits. I therefore respectfully suggest that Congress consider the following:

1. *Improvements in State Drivers' Licenses.* This is the principal identity document in our country. We must eliminate the ability of people to falsely assume the identity of another. Indeed, some of the September 11 terrorists facilitated their actions through easy access to Virginia drivers' licenses. The only way to prevent identity fraud

is to include biometric data on the card, such as a finger print. (Indeed, it is my understanding that California uses retinal scans for commercial drivers' licenses.) In addition, minimum nationwide issuance standards should either be imposed by Congress or agreed upon by the states. Both changes would be minimally intrusive to the average American and yet would dramatically increase the reliability of this document.

2. *Expanded Employer Access to INS and Social Security Databases.* Congress should expand the "Basic Pilot" computer database to employers in every state in the nation. The benefits of Basic Pilot are only available today to employers who have at least one office in one of the five following states: California, New York, Texas, Florida or Illinois. Employers in all states should have access to this database. In addition, the Social Security Administration should be appropriated more funds and directed to improve the accuracy of this database in order that the "true identity imposters" may be detected.

3. *Improvements to Birth and Death Records.* The vulnerability of our birth certificate system allows aliens to bypass the immigration system altogether and impersonate U.S. citizens. The Jordan Commission recommended in 1994 that we "reduce the fraudulent access to so called 'breeder documents,' particularly birth certificates, that can be used to establish an identity in this country." The specific steps recommended by the Commission included: (1) regulation of requests for birth certificates through standardized application forms, (2) a system of interstate and intrastate matching of birth and death records; (3) requiring that federal agencies only accept certified copies of birth certificates; (4) using a standard design and paperstock for all certified copies of birth certificates; and (5) encouraging states to computerize birth

records repositories. I think these recommendations are sensible, practical, and should be enacted. It is time.

I appreciate this opportunity to share my views and look forward to answering any questions.

Mr. HORN. We now go to Mr. McCollum, who during my years in the House, no one was a better legislator than he was, and we're glad to have you back here. Mr. McCollum.

Mr. MCCOLLUM. That's a high compliment, Mr. Chairman, and I'm very glad to be back here too today with you, and especially pleased to be with this distinguished panel, my friends, Speaker Gingrich and Senator Simpson, with whom I've served a number of years, and on a topic that really is very timely and very important. I know like everybody here, that we all were affected terribly by this tragedy on September 11th, the attacks on us that I think most of us envisioned was unimaginable.

Even many of us who served in the arenas that I did in Congress knew that sooner or later we were going to have a terrorist attack of some magnitude, we could not have expected nor anticipated the horror that came with this particular one, and now we're having a reaction to that. Having been chairman of the Crime Subcommittee and, having chaired the Subcommittee on Human Intelligence, founded the Terrorism Task Force, been—18 of the 20 years served on the Immigration Subcommittee, many of those years with Senator Simpson's work and mine, together with the fellow up there you mentioned, Brooks and others. I come to this with a perspective of absolute conviction about a couple of things.

One of those is that there is no need for a national ID card and I'm very much opposed to one, but I think it's important to identify what a national ID card is. What do we mean by that? Mr. Chairman, I mean by that, a uniform system, a uniform card that every American would be required to carry to produce to law enforcement employers, various government agencies for identification purposes. Such a card would contemplate a national data base, access by a computer for verification purposes. It might contain a strip on the back like your Visa card does. It has data and information already built in it or accessible through a computer. A photograph, a fingerprint, possibly even a national data base that every American had a fingerprint in. I don't favor that. I don't think that's right. I think that's an insult to our system of government, the privacies and those that our great freedoms that our founding fathers envisioned. It's a Big Brother-type system.

But we do need to make some of the identifiers we already have work, and that's what all of us are testifying about today. I have not heard a word that either of my colleagues said that I took umbrage with, but I do have a perspective on a couple of these a little bit differently.

First of all, I believe that the Social Security card desperately needs to be made more secure. There's been great resistance to doing much with that card over the years but back in 1996 or, excuse me, 1986 when the Simpson-Mazzoli, and then more in the amendments of 1996 in the immigration world for employer sanctions, and when you go to get a job, the two principal identifiers became narrowed down to your driver's license and your Social Security card.

So if you can produce them fraudulent or otherwise today, they essentially get you a job and the Social Security card, as well as the driver's license, is commonly used for a whole host of other identification purposes today. Yet it is probably the most fraudulently produced document in America. It is a document that has been flimsy in paper for years.

In recent years, the Social Security Administration has put a few fibers in it but by no means made it tamper resistant or counterfeit-proof. And I encourage this committee and other Members to really take a look at a proposal that I have in as a legislative matter for a good number of Congresses.

One that was—is attached and submitted to this testimony today, H.R. 191, and a bill in the last Congress, Mr. Chairman, that you were an original cosponsor of. That is a proposal that would require the Social Security Administration to make the Social Security card as secure against counterfeiting as a $100 reserve notice with a rate of counterfeit detection comparable to the $100 reserve notice and as secure against fraudulent use as a U.S. passport. We're not talking about putting pictures on the card, we're not talking about any of that, but it's all those interwoven things that you can use, use ultraviolet lights and so forth to determine.

I also would encourage the same type of activity that has been discussed here today with regard to the driver's license. I think that driver's licenses at least the general standards for what they are should be uniform throughout the country, and I don't think we have to mandate that. I don't think Congress should preempt the States, but I think that there should be an effort to encourage that from Congress and I think that it should be done in a way that does have either a uniform standard proposed or you get the States together to do that or whatever. All driver's licenses should certainly have photographs on them, they should have the signature on them. They should have a fingerprint or another biometric identifier on them, and they should have holograms and other types of devices built into those driver's licenses just like I suggested for the Social Security card so they cannot be easily reproduced and so that when you take it somewhere to an employer or to a person who's law enforcement, they can be quickly checked. You know, we have a little machine that's been around for a number of years on fingerprints. You put it on this desk—I've had it come when I was chairman before my committee. You probably have too, Mr. Chairman.

And it's not—doing nothing more than saying if you put your finger on that machine and you put the card that you have with your preexisting fingerprint on it, it matches it or it denies it, and it doesn't have to go to some central data base to do that. And at least that will tell me biometrically whether the person I'm looking at is the same as what's on that card. I also concur with the view that we need to do something about birth certificates. One of the great, great problems in this country are the breeder documents that Senator Simpson has talked about and that's important.

Last, I want to comment on one aspect of the Immigration Service because I do believe that the focus rightfully should be there, as Congressman Castle stated in his opening. There is a great, great opening right now in this country for people to come here and not be identified. We need a tracking system. We need to be—we need to find people so we don't have visa overstays, and we need to shore up so many things. A number of things have been mentioned, but one has not been. Today when somebody goes before a formal proceeding of an immigration tribunal or to the Immigration Service or whatever, they're usually released on their own recognizance or maybe on a cash bond. The Immigration Service has the authority to have a security bond, much like a bail bond, but they don't do that, and I believe that it would be extremely helpful to get people to show up when they're supposed to before immigration proceedings. If there was a general policy that a security bond be used and then have the private sector, bail bondsman, if you will, like they do in criminal law, be responsible for bringing them in, making sure they do show up because people can come not only to this country and get here too easily because of the visa system and visa fraud if we don't track them, but then when they do show up to a proceeding and they're supposed to come back in 90 days or 6 months or whatever, we have no system to bring them back in. We have no way of knowing where they are and we don't have nearly enough police or immigration officers that will ever be able to do that.

So why aren't we using the private sector the same way that we do in criminal law? It's not being done today. So I would encourage that this committee and your members look very strenuously at not only making these identifiers more secure and finding ways to track visa overstays and people who come in here, but making sure that when they're here, that is, those who are aliens, show up when they are supposed to at the end of whatever period of time that there is.

Thank you, Mr. Chairman.

Mr. HORN. Thank you for your testimony.

[The prepared statement of Hon. Bill McCollum follows:]

TESTIMONY OF THE HONORABLE BILL McCOLLUM

former Member of Congress, (Florida 8th District)

before the

Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations
Committee on Government Reform
U.S. House of Representatives

Friday, November 16, 2001

Mr. Chairman, I appreciate the opportunity to testify before the Subcommittee on the question of whether the United States should have a national identity card for all citizens, resident aliens and others who are residing in this country.

All of us are deeply disturbed and moved by the tragedy of this past September 11. Terrorist acts of this magnitude on American soil seemed unimaginable to most people. They were shocked to learn that the Al Qaeda operatives who commandeered the planes and flew them into the World Trade Center Towers and the Pentagon had been planning and preparing for these attacks while living in the United States for a considerable amount of time and were never suspected by any of our intelligence or law enforcement community. One of the natural reactions to this has been a clamor for changes in our laws and practices to try to make sure that such terrorists can't come here from abroad in the future and operate so freely and undetected. As part of this effort, some have revived the idea of a national identification card, which is the subject of this hearing.

As you may recall, for a number of years before leaving Congress this past January I chaired the House Subcommittee on Crime and at the same time chaired the Subcommittee on Human Intelligence, Analysis and Counterintelligence. For six or seven years prior to going on the House Intelligence Committee in 1995, I was the founder and chairman of the House Task Force on Terrorism and Unconventional Warfare. And for eighteen of the twenty years I served in Congress, I was a member of the Subcommittee on Immigration. In short, I probably spent as much or more time studying terrorism, aliens and identification issues than any other past or present member of Congress. This doesn't mean I have all the answers, but I have some definite opinions I want to share with you.

There is no need for a national identification card, and I am personally opposed to establishing one.

By national identification card I mean a uniform card that every American citizen and every resident alien and probably a number of categories of non-resident aliens present here are required to carry and produce to law enforcement, employers, various government agencies, etc., for identification purposes. Such a card contemplates a national data bank on everybody living in the United States which can be accessed by computer for a variety of verification purposes. Such a card might contain a strip on the back like a Visa or MasterCard that allows an instantaneous electronic check into the data bank, and it might have the person's photograph and fingerprint. In a really sophisticated system, everybody's fingerprint would be electronically on file in the national database and with the fingerprint on the identification card there could be an instantaneous check to corroborate that the person presenting the card is the person on file and is who he says he is.

This kind of Big Brother national identification system is offensive to me, contradicts some of our most sacrosanct American principles of personal liberty and expectations of privacy and is far in excess of what is needed to provide us with the security and protections we all want.

But we do need to make the Social Security card and our drivers' licenses more tamper-resistant and counterfeit-proof. Both these documents, outside of passports and green cards, are the most commonly used identification documents in America. When we go to airports, write checks or a whole host of other things, we are frequently being asked for our drivers' licenses. And whether we like it or not the Social Security number is frequently used to corroborate that we're who we say we are. Following the enactment of the Simpson-Mazzoli immigration bill in 1986, and even more so since the 1996 amendment, the most commonly used and statutorily acceptable form of identification employers use to verify a person's right to employment is a combination of a driver's license and a Social Security card.

I doubt there is any document in America more fraudulently produced than a Social Security card. The Immigration and Naturalization Service (INS) has long expressed frustration with and pretty well given up on trying to enforce employer sanctions for knowingly hiring an illegal alien because of document fraud. The principal culprit is the Social Security card. In recent years the Social Security Administration (SSA) has put some security protection threads in newly issued Social Security cards, but it has resisted efforts to make the Social Security card as tamper-resistant as the paper of a passport or as counterfeit-proof as the $100 bill. Furthermore, there has been no interest shown in reissuing more secure Social Security cards to anyone who has an older version with no security threads, etc.

In recognition of this problem, I introduced and re-introduced in several Congresses legislation to require the Commissioner of Social Security to make the card as secure against counterfeiting as the $100 Federal Reserve note, with a rate of counterfeit detection comparable to the $100 Federal Reserve note, and as secure against fraudulent use as the United States passport. A copy of the most recent version of this from the 106th Congress, H.R. 191, has been submitted to the Subcommittee as part of my testimony. Mr. Chairman, you may recall that you were an original co-sponsor of this legislation.

It should be noted that H.R. 191 contained an express provision which read, "**NOT A NATIONAL IDENTIFICATION CARD – Cards issued pursuant to this section shall not be required to be carried upon one's person and nothing in this section shall be construed as authorizing the establishment of a national identification card.**" The bill also contained the language, "**NO NEW DATABASES – Nothing in this section shall be construed as authorizing the establishment of any new national databases.**"

If somebody presents a Social Security card today to anyone for whatever purpose, it is very unlikely that the person to whom it is presented can verify it's a real card as opposed to a fraudulent document. For somebody in the business of making false Social Security cards, it's not too hard to find a match of a real person's name with his or her Social Security number, and since there is no photograph on a Social Security card or other form of identifier to let somebody know the card belongs to the bearer, anyone to whom it's presented in trying to verify it would only get corroboration that the Social Security number matched the name given. So this makes it extremely important that the Social

Security card itself be made tamper-resistant and counterfeit-proof. Then with the proper equipment, the person to whom it is presented can verify on the spot the card's authenticity and make the verification of a name/number match meaningful.

One reason why immigration law for employment verification requires the presentation of both the Social Security card and a driver's license is because the Social Security card bears no photograph and the driver's license alone would not necessarily demonstrate a person's legal status in the country or eligibility to work. But for the document fraud problem, the combination of Social Security card and drivers license is a potent one for identification purposes, and there is no need for a national identification card or national data bank.

While I do not favor a federal mandate on the states or preemption of state laws, it would be preferable if all states adopted a set of uniform guidelines for drivers' licenses. There should be a photograph, a signature, at least one fingerprint and as many counterfeit-proof/tamper-resistant features as is reasonably possible. Without imposing requirements on the states, it might be useful for Congress to promulgate a proposed uniform set of standards for driver's licenses or to call for a commission from the governors of the various states to create a uniform standard.

With a fingerprint on a driver's license, it is possible for the person to whom it is presented for identification to corroborate on the spot with the proper machine that the person presenting the card is the same as the person who gave the fingerprint that's on the card. This would not require the keeping of any fingerprint database, but rather would be possible with the use of existing equipment that could sit on a small space on a desk and be used to match fingerprints instantaneously.

America is the greatest free nation in the world. We must do everything possible to keep it that way. The genius of our Founding Fathers in writing our Constitution and the Bill of Rights lay in the careful construct of checks and balances they established. They had felt the strong hand of King George and were determined to make sure that the new government they were creating protected against unnecessary intrusions of the state and allowed for the maximum personal freedoms. They recognized, as we must now, there must be the right balance between the needs of our people to be secure and safe in their homes, in their neighborhoods, at work and at school and the need to protect our freedoms from unnecessary government intrusion for such intrusions can take away the very essence of liberty which has been the hallmark of the Nation.

A national identification card upsets that balance. Making the Social Security card and drivers licenses counterfeit-proof and tamper-resistant serves our identification needs in these troubled times without crossing that line.

Much of the concern I have today with our domestic security centers on the laxity of our immigration laws and procedures. Other than making immigration documents counterfeit- and tamper-proof along with the improvements to the Social Security card and driver's license, the two things we really need to do in this theater are improve our screening procedures for issuing visas to screen out people who shouldn't be getting in and create a tracking system of aliens in this country that really works.

When someone enters this country as a visitor or as a student or for whatever reason other than a permanent resident-alien, they are here for a specified amount of time with a clear expiration date on it. It is absolutely essential to our security that whatever resources are necessary be put into a tracking system that keeps these people from just disappearing into our society and only appearing in immigration proceedings out of the goodness of their heart or because they happened to run afoul of our law in some other way. As you know we don't have an effective computerized visa overstay program. And not only that, we don't really have a good tracking program or system to assure the appearance of people who make immigration court or other INS official appearances in proceedings that may lead to their exclusion or deportation. The vast majority of aliens who make formal appearances in proceedings are released on their own recognizance or on a cash bond; it is very rare that a surety bond is used. It would make a lot more sense if our immigration officials put to use the surety bond system like we use in our criminal laws with bailbondsmen. That way the private sector could go to work for the government to assure the appearance of a lot more of these aliens than presently come forward at the appointed times. Things like this plus improving our intelligence capabilities are where the focus should be, not on a national identification card.

Again, there is a tremendous need for tamper-resistant and counterfeit-proof Social Security cards and drivers' licenses and uniformity among our drivers' licenses throughout the fifty states. But it would be an insult to our personal freedoms in this country and totally unnecessary to adopt a national identification card with its accompanying national data bank.

Thank you for letting me appear today and give you my thoughts.

To improve the integrity of the Social Security card and to provide for criminal penalties for fraud and related activity involving work authorization documents for purposes of the... (Introduced in the House)

106th CONGRESS
1st Session
H. R. 191

To improve the integrity of the Social Security card and to provide for criminal penalties for fraud and related activity involving work authorization documents for purposes of the Immigration and Nationality Act.

IN THE HOUSE OF REPRESENTATIVES

January 6, 1999

Mr. MCCOLLUM (for himself, Mr. BEREUTER, Mr. BILBRAY, Mr. CAMPBELL, Mr. CUNNINGHAM, Mr. HORN, Mr. HUNTER, Mr. ROHRABACHER, Mr. SHAYS, Mr. SHERMAN, Mr. STARK, and Mr. STENHOLM) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committee on Ways and Means, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To improve the integrity of the Social Security card and to provide for criminal penalties for fraud and related activity involving work authorization documents for purposes of the Immigration and Nationality Act.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. PROTECTING THE INTEGRITY OF THE SOCIAL SECURITY ACCOUNT NUMBER CARD.

(a) IMPROVEMENTS TO CARD-

(1) IN GENERAL- For purposes of carrying out section 274A of the Immigration and Nationality Act, the Commissioner of Social Security (in this section referred to as the `Commissioner') shall make such improvements to the physical design, technical specifications, and materials of the social security account number card as are necessary to ensure that it is a genuine official document and that it offers the best possible security against counterfeiting, forgery, alteration, and misuse.

(2) PERFORMANCE STANDARDS- In making the improvements required in paragraph (1), the Commissioner shall--

(A) make the card as secure against counterfeiting as the 100 dollar Federal Reserve note, with a rate of counterfeit detection comparable to the 100 dollar Federal Reserve note, and

(B) make the card as secure against fraudulent use as a United States passport.

(3) REFERENCE- In this section, the term `secured social security account number card' means a social security account number card issued in accordance with the requirements of this subsection.

(4) EFFECTIVE DATE- All social security account number cards issued after January 1, 2002, whether new or replacement, shall be secured social security account number cards.

(b) USE FOR EMPLOYMENT VERIFICATION- Beginning on January 1, 2008, a document described in section 274A(b)(1)(C) of the Immigration and Nationality Act is a secured social security account number card (other than such a card which specifies on the face that the issuance of the card does not authorize employment in the United States).

(c) NOT A NATIONAL IDENTIFICATION CARD- Cards issued pursuant to this section shall not be required to be carried upon one's person, and nothing in this section shall be construed as authorizing the establishment of a national identification card.

(d) NO NEW DATABASES- Nothing in this section shall be construed as authorizing the establishment of any new databases.

(e) EDUCATION CAMPAIGN- The Commissioner of Immigration and Naturalization, in consultation with the Commissioner of Social Security, shall conduct a comprehensive campaign to educate employers about the security features of the secured social security card and how to detect counterfeit or fraudulently used social security account number cards.

(f) ANNUAL REPORTS- The Commissioner of Social Security shall submit to Congress by July 1 of each year a report on--

(1) the progress and status of developing a secured social security account number card under this section,
(2) the incidence of counterfeit production and fraudulent use of social security account number cards, and
(3) the steps being taken to detect and prevent such counterfeiting and fraud.

(g) GAO ANNUAL AUDITS- The Comptroller General shall perform an annual audit, the results of which are to be presented to the Congress by January 1 of each year, on the performance of the Social Security Administration in meeting the requirements in subsection (a).

(h) EXPENSES- No costs incurred in developing and issuing cards under this section that are above the costs that would have been incurred for cards issued in the absence of this section shall be paid for out of any Trust Fund established under the Social Security Act. There are authorized to be appropriated such sums as may be necessary to carry out this section.

SEC. 2. CRIMINAL PENALTIES FOR FRAUD AND RELATED ACTIVITY WITH WORK AUTHORIZATION DOCUMENTS.

(a) IN GENERAL- Section 1028 of title 18, United States Code, is amended--

(1) in subsection (a)--

(A) in paragraphs (1) and (2) by striking `an identification document or a false identification document' each place it appears and inserting `an identification document, false identification document, work authorization document, or false work authorization document';

(B) in paragraph (3) by striking `identification documents (other than those issued lawfully for the use of the possessor) or false identification documents' and inserting `identification or work authorization documents (other than those issued lawfully for the use of the possessor) or false identification or work authorization documents';

(C) in paragraph (4) by striking `an identification document (other than one issued lawfully for the use of the possessor) or a false identification document' and inserting `an identification or work authorization document (other than one issued lawfully for the use of the possessor) or a false identification or work authorization document';

(D) in paragraph (5) by inserting `or in the production of a false work authorization document' after `false identification document'; and

(E) in paragraph (6) by inserting `or work authorization document' after `identification document' each place it appears;

(2) in subsection (b)(1)--

(A) by striking `an identification document or false identification document' in subparagraph (A) and inserting `an identification document, false identification document, work authorization document, or false work authorization document';

(B) in subparagraph (A)--

(i) by striking `or' at the end of clause (i);
(ii) by inserting `or' at the end of clause (ii); and
(iii) by inserting the following new clause after clause (ii):
`(iii) a work authorization document;'; and

(C) by striking `identification documents or false identification documents' in subparagraph (B) and inserting `identification documents, false identification documents, work authorization documents, or false work authorization documents';

(3) in subsection (b)(2)(A) by striking `a false identification document;' and inserting `a false identification document, work authorization document, or false work authorization document;';

(4) in subsection (c)--

(A) by striking `identification document or false identification document' each place it appears in paragraph (1) and inserting `identification document, false identification document, work authorization document, or false work authorization document'; and

(B) by adding `work authorization document, false work authorization document,' after `false identification document,' in paragraph (3); and

(5) in subsection (d)--

(A) by striking `and' at the end of paragraph (5);

(B) by striking the period at the end of paragraph (6) and inserting `; and'; and

(C) by inserting after paragraph (6) the following new paragraph:

(7) the term `work authorization document' means any document described in section 274A(b)(1)(C) of the Immigration and Nationality Act.'.

(b) CONFORMING AMENDMENTS-

(1) IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT- Section 4(b)(2) of the Identity Theft and Assumption Deterrence Act of 1998 (Public Law 105-318; 112 Stat. 3010) is amended by striking `or false identification documents' and inserting `false identification documents, work authorization documents, or false work authorization documents'.

(2) HEADING- The heading for section 1028 of title 18, United States Code, is amended to read as follows:

`Sec. 1028. Fraud and related activity in connection with identification and work authorization documents and information'

(c) CLERICAL AMENDMENT- The item relating to section 1028 in the table of sections at the beginning of chapter 47 of title 18, United States Code, is amended to read as follows:

`1028. Fraud and related activity in connection with identification and work authorization documents and information.'

Mr. HORN. And we'll now go to questioning. It's going to be 5 minutes per person because of the travel schedules, and we will alternate between the majority and the minority, and I will start it off. And if Mr. Chief Counsel will get the technology here, we're in business.

In my opening statement, I cited a Pew Research Center study that showed overwhelming support, 70 percent of those polled for a national identity system, and are all of these people just misguided? How do you feel? Do you think from what you have seen of just the average citizen when you get into a debate like this? And I would take it with this particular three of you, would you have, say, a hardened, if you will, Social Security or would you take the license which, in my case with California, they have a photo and they have a thumbprint, and not all of them do it, but that's pretty good identification.

So any other types you're talking about than simply hardening up the Social Security card and then putting a picture on it or a thumbprint. I remember the supervisors of Los Angeles County, which is a county of 10 million people and they started with the photo on the welfare situation and a few thousand people got off the rolls because they were going two, three, four places to get money, and that was one way to do it.

Mr. MCCOLLUM. Well, Mr. Chairman if I might respond to that, I don't believe that, for example, in the Social Security card, you want to go to put a picture on it, I don't think you need to. I think you can stay paper. Its purpose is to make sure that the number that's on that card and the name on that card are the bearers. When you take that card and produce it for whatever purpose, that simple fact can be verified.

I also think, by the way, that it would present problems in reissuance. The Social Security card, one of the great reasons why that's been a problem in getting it corrected is the Social Security Administration wanted to go to the cost of reissuing a lot of cards. They don't have to reissue all of them. But I think they do need to reissue those with those younger age groups and that would be an added expense I don't think you'd want to encounter. And again I don't think we need a national ID card as such, a separate card, if you have a driver's license and a Social Security card; one with a picture, one without it are more secure, more tamper-resistant and counterfeit-proof.

Mr. HORN. Mr. Simpson.

Mr. SIMPSON. It's interesting, Mr. Chairman, that polls throughout the Select Commission back in the 1980's, 1985, 1990, if you'd asked the American people, Gallup, whatever, if they favor restrictions on immigration, 70 percent do. It just stays that way. Not illegal or—I mean, I'm talking about legal and illegal immigration. Interesting. But when you come to the Congress, it doesn't get done that way because the Statue of Liberty suddenly enters the phrase and all of us are children of immigrants. Mine are from Holland, orphans. If my granddad hadn't killed a guy in the middle of the main street, we'd have had a better reputation there in our State, but that's another story and I won't go into it.

Nevertheless, you can't continue to talk about the Statue of Liberty again. You must talk about reality and all three of these—all three of us I think are, all of you are, but I think the one that surprised me was when they put the examination into California for the retina exam on truckers, guys just stood outside the building because they didn't want to go through any part of that because they'd been using fake ID's and all the rest of it. It was a very serious problem, and I think you ought to look into that California commercial driver's license issue retinal exam.

Mr. HORN. Thank you.

Mr. GINGRICH. I think that what you have to recognize is that the people most opposed to a national ID card are dramatically more passionate than the people who have some vague general support for a national ID card. And that's why I think Senator Simpson was right early on in saying that if we go down that road, it's a dead end. It won't happen. On the other hand, most Americans, I think, can be led to agree that having an efficient transfer of information so you know that your driver's license is real, that it's valid, so you can check it across State boundaries, and for specific purposes.

Foreign visitors, I think most Americans would agree, you could have a nationwide system of identifying—because that's not part of what we think of as our civil liberties. People that have very important security jobs, whether it's on airports or elsewhere, people would agree you ought to have a pretty high standard of security because they understand that's a function of your job, it's not an infringement on civil liberty, but I would encourage you to be minimalist in this. You want to get to a highly secure system that is across the whole country, that is ideally mostly decentralized in terms of States implementing it, but with information able to flow across State boundaries and you want to do everything you can to minimize the threat to those whose primary concern is civil liberties.

Mr. HORN. Thank you. My time is up.

Five minutes to Ms. Schakowsky, the ranking member.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

Following up on that minimalist approach and using your example, Speaker Gingrich, of what happened before September 11th, that the CIA actually transmitted information to the FBI and it never got through, what I am wondering is are there not systems in place were we to have the proper technology for sharing that system—that information that could provide the kind of security we need?

That is the question, but let me just say that in many, many hearings that we have had since September 11th, what we have found is that information was all over the place, and that had it only been shared and gotten to the right place, that we could have done this or that to prevent what happened. And so I am just wondering if it isn't a matter of looking at our systems, adding new technologies where we need to, but not new authorities to gather that information; if it is just a matter of making more efficient what we already have.

Mr. GINGRICH. I think you are 90 percent right, but the 10 percent is missing, I think, could kill us, and let me describe what I mean. First of all, whatever system we build, we ought to have a competitive team try to break and find out how rapidly can you buy a counterfeit. How rapidly can you figure out a way to work around it, because we have active opponents who study what we do and who could spend 2 or 3 years trying to penetrate our systems. And if we are really serious about security, then we ought to be serious about learning what its weaknesses are.

Second, as Senator Simpson said a minute ago, we discover that whether it is illegal aliens or it is people who are for one reason or another using a false identity, that there are—even in the current system, even if you had 100 percent accuracy of sharing the information, some of the information going into the system is false, and we don't have today the kind of identifiers and the kind of structure to make sure that the information you put in is accurate information. I think that would be the other zone where I think there has to be serious work done.

But I yield to my colleagues.

Mr. SIMPSON. Congresswoman Schakowsky, you are right on track. One of the most frustrating things for me and I know for Peter Rodino and Ron Mazzoli and all the rest of us was the absolute stubbornness of the agencies to share information. The one that appalled me was Customs and INS—oh, there is a real internal—it was bizarre. It was childish. Customs—Customs can pick up a lot of stuff. They know what is going on, and they'd share it, and they'd say, we handle that. The Border Patrol and the INS and the Justice Department and the CIA and FBI and oftentimes their arrogance and the CIA's secret arrogance, I mean, this is where you have to smash the big bug right here. And I think that is what I hear the President saying that he's going to give Ridge all the authority to do that, and he's going to make him do it. Well, we have all been here a long while. Merry Christmas. We will see what happens.

Mr. MCCOLLUM. I know that's a big problem. What Senator Simpson just said, and we joked about it, it's so true. If Tom Ridge can do it—I see the other day where he's talking about maybe merging the Border Patrol, Customs and the Coast Guard. I think that is going to be an awfully big hill to climb. And you'd be better off using the energies you have got to do things like forcing the Social Security Administration to really go out and make the card tamper-resistant; make it like the $100 bill; take the driver's license and make it more secure; take the ideas that Newt Gingrich just said about putting a data base together nationally to talk to each other on these things technically and then cajole, continue to cajole, the agencies to do this.

Ms. SCHAKOWSKY. Let me ask one quick other question. One of the problems created by drivers' licenses becoming de facto national identification systems is the privacy protection of those records is very poor. We know that States often sell that information to—along with the person's address, and it becomes out there in the public. How can we make sure that any particular system we use doesn't mean that information is sent out? And should Congress stop the validation of Social Security numbers until the States institute—a State instituted privacy protection for drivers' license records, because they often check those drivers' licenses against Social Security cards?

Mr. MCCOLLUM. Well, Ms. Schakowsky, I don't think we should stop the validation system as it exists because we have a security problem right now, and we need to let these things happen as best we can. But I do believe that Congress should be concerned and should encourage States to make the right decisions to protect the privacy of the data that is in the data base. That is the real point I made about not wanting a national ID and trying to define it for you. The thing the American public may say when they say, "We are all for a national identification card," is one thing, but when they really get down to it, nobody that I know of favors a Big Brother data base somewhere, whether it is in the State or the Nation, where other people can get access to your personal information. And there is a huge difference between providing a chance, for example, for somebody who is an employer or law enforcement to call up or do whatever we can on the computer to a data base and say, if you walk in, that this is my name and this is my Social Security card, and verify that they both match electronically. There is a big difference between that and somebody walking in and saying, "OK, I have got a name, now let me go find out what is the Social Security number, tell me," or the other way around. "I got a Social Security number, you tell me the name that goes with it."

We don't want that information shared publicly, and that's the kind of thing that you need to discriminate, in my judgment, against. But you are not going to mandate that in one big piece of legislation. It is going to take a lot of work to get understanding on the part of each person or group in the States that are making those decisions to make them be aware of what they're doing and be more secure to educate.

Mr. SIMPSON. May I add one thing? Newt Gingrich is a wizard of the keyboard, and I am not adept in technical prowess of the electronic age, but I do share with you, I believe totally, there really is no such thing as privacy anymore because of the information technology. They have got you in every data base in this country, Social Security, driver's license, organ donor, blood type, you name it, FBI reports. I used to read them. And with what's happened with information technology in this country, I think privacy is gone.

Mr. HORN. And now I yield 5 minutes to the gentleman from Florida Mr. Miller and then Mrs. Maloney.

Mr. MILLER. Let me followup on what Senator Simpson brought up, and that's the issue of privacy. And I know Speaker Gingrich and Mr. McCollum worked this issue when they served here in financial privacy and medical privacy, and I know you wrestled with trying to get legislation through. Would you comment on that experience and what the experience has been that you are aware of controlling that kind of privacy, because we are all public figures, and you were public figures when you served here in this institution, but that is really one of the core concerns here is privacy. And when you wrestle with it, and we pass legislation on financial, medical in particular, is it working, and what can be done to assure privacy if we move to some type of ID?

Mr. GINGRICH. I think this is an extraordinarily important issue in the way big computers is a much bigger danger than Big Brother. It is so seductively convenient. You use a credit card. It doesn't occur to you how much information you are building on that credit card every week when you charge things, what it tells somebody who is clever about your habits, your interests, your taste, etc. Then you go and use telephones, which have records, and then you go and pump gasoline. And then you go and you get a driver's license—I mean, by the time you are done with all this, if you were to accumulate all the information that currently exists about you, you'd be stunned at how much you are a public person in ways you did not intend.

And I think there are two very different layers of this. We badly need to think through an integrated privacy policy in terms of law. As I said earlier, I am a passionate believer in electronic medical records, but I'm also a passionate believer in a Federal law that would make inappropriate misuse of that information a felony and have very stiff penalties. We have to have the information, but we want to protect people from having it exploited to hurt them.

Similarly, I think that it is important to recognize, and as I stated in my own testimony earlier, I want to commend the subcommittee again, you know, for your report issued last week that the Federal Government agencies have security levels that in many cases are so laughable that any really competent sixth-grader could break into them. And even the ones that are relatively secure, except for the top two or three, a relatively competent junior-high-schooler could break into them.

And I think it's really important to understand—and I met recently with the National Association of State Chief Information Officers, and we talked about the fact that we need to set a whole new standard against hacking, against organized crime, against terrorists, against foreign governments that want to try and break in, and recognize that is going to take a sharing of technical knowledge. It's just not writing laws, but understanding how to write these security systems. And we have to recognize how much of our code is now written outside the United States. And I think we have to have a project between the Department of Defense, the National Science Foundation and the National Security Agency to really figure out a way to literally scan all the code we now rely on, because we don't know how many various back doors have been built in, because you are talking about millions of lines of code that routinely now enter the U.S. system from overseas.

Mr. SIMPSON. May I say, too, sir, and to the panel, who knows more about the loss of privacy than all of us? You? Me? All of us who are in public life have none—and maybe that's all right. It's all right with me. I laid it out there, all the peccadillos and all the goofy things I ever did. But there is no privacy for a public figure. So I think it is very important to realize that as we do these things, the media loses a lot of sleep about us because when we get active, they go into everything we've ever done: first grade, high school, college, the whole works, and we get the whole load. When you come back to them and say, aren't you intruding on our privacy? And they say, well, you are public figures, and we are not. I say, more guys know you on that tube than know us—all of us in Congress, so don't give me that. I think we ought to know a little bit about your private life.

It's a sick idea, I know. It's about the first amendment. It belongs to me, too. We are the ones that suffered the slings and arrows. And I am ready to do that at any time, in fact, in anything, anything—and the woman I have been living with for 47 years is sitting back here—in anything they couldn't dig up on Al Simpson, but let me tell you, they sure as hell tried.

Mr. MCCOLLUM. I would like to make a distinction, Mr. Miller. You asked about privacy, and I think what is a person's reasonable expectation, what are the Constitutional protections for that, and there are some. And we live in a different age when it comes to the computer, but we need to divide up what people should reasonably expect in the way of privacy, with respect to privacy and their government intrusion into that, and what they can reasonably expect when they go out and take certain steps on their own in the world of business and with data that they freely yield to someone. Two different things.

The privacy that is protected in the Constitution clearly is there when it comes to the government coming into your house, not just from a criminal law standpoint, but an unreasonable search and seizure or eavesdropping or whatever, and we have all kinds of checks on that, and they should always exist. When it comes to the computer, when you use the computer, you need to be aware you are opening up whatever you put in there for other people to look at. And we can talk about trying to restrict that all we want, and it is very difficult to do. On the other hand, when you give up data to a bank, which is where we first met the privacy issue in the last Congress and it created a lot of hullabaloo, I don't think people were even thinking about the privacy question so much there, but the reality is prior to the enactment of the big bank bill last Congress, banks could share data they had with anybody. There were no restrictions, and we put the first restrictions—Congress did in the law. And those restrictions said that since we allowed the merger of the operations of banks and security companies and insurance companies, that if you were in the same holding company, you know, the same group, within that group, financial information that you as a citizen gave to that bank could be shared. But if they wanted to go out and give that information out to somebody that wasn't a party to their company, to their holding company, they had to seek your permission. And those are the kinds of things we need to think about at each stage.

You give up your rights when you go and do a certain business transaction, but you should be informed what you are giving up. And before information that is given by you to a business or third party is given away to somebody else, you should have a right to say yes or no. But absolutely you should have a reasonable expectation that the government won't intrude your privacy. That is sort of the broad guidelines. It is a huge subject, but that is the guideline.

Mr. HORN. Thank the gentleman, and now 5 minutes for the gentlelady from New York Mrs. Maloney.

Mrs. MALONEY. Thank you, Mr. Chairman.

Speaker Gingrich, you mentioned that you are not supportive of a national ID card, but you support a more sufficient transfer of information. Since all of the known terrorists were visitors with visas here either legally or illegally, it appears that a good place to start would be with a more thorough tamper-proof green-card; would you agree?

Mr. GINGRICH. I did say earlier that I drew a very sharp distinction between the need for a national system for non-citizens, which I think should be administered by the Federal Government, run across the whole system; should have a clear identifier that is biometric; and should have a data base that can be accessed by a variety of agencies. And that should be a condition of being here.

I also said, and I think you get real controversy about this, but I think we are much better to go to some kind of guest worker program and accept the legality of people who are here for the purpose of working and get them identified. I think when you have a pool of—I think the numbers are 3 to 5 to 7 million people who are illegally here, but are here to do legal things—they are not here to be drug dealers or terrorists, that pool of people who are outside the system causes, I think, a real challenge for security purposes. So I think it would be much healthier to have an identifiable guest worker program and simply have a requirement that everybody who is a non-citizen have some kind of an identifier and a sophisticated greencard with a central data base. That should be national. And my guess is overwhelmingly the American people would support that.

I am also suggesting if you come here as a visitor as part of the transit point, then we ought to have some biometric, an iris or retina scan, so we can determine whether or not you are a person who is a threat to the United States at a point of entry, even for visitors who are here on business or here for tourist purposes. And my guess is that most people on the planet—people who come for business or vacation want to be safe, and they want a safe system, and as long as it is not too intrusive, I think they would be very accepting of that kind of safety.

Mrs. MALONEY. Building on that base of a non-citizen data base that is national, who should maintain this data base? Where would you put it in government? Would you put it in the INS? Would you put it in the FBI? Would you put it in the new Homeland Security?

Mr. GINGRICH. I am going to yield to my two colleagues. I haven't thought about it where in the Federal Government you would house it. I would probably outsource a great deal of management of it, because I think it is very, very hard for the Federal Government to get first class——

Mrs. MALONEY. It has to be maintained by the Federal Government.

Mr. MCCOLLUM. It is the Immigration Service you are talking about.

Mrs. MALONEY. You say INS.

Mr. SIMPSON. It was my experience, Congresswoman Maloney, I met some of the finest people in both parties who were Commissioners of the INS. It is an absolutely unwieldy agency. Doris Meissner did her best. There's nothing you can do with them. The regional people are tough. The district people, they are all—it has got to be done there. If you go ahead with the legislation that is being proposed, then it would be the INS, which would be logical, not Social Security.

Mrs. MALONEY. This is only for non-citizens.

Mr. SIMPSON. Yes. And many non-citizens hold Social Security cards.

Mrs. MALONEY. I would also like to ask our panelists, who do you believe should have access to that data base, assuming it is in INS with oversight by——

Mr. GINGRICH. For verification purposes, it is reasonable to ask people to prove who they are when they apply for a job if they are a non-citizen, and I think I would allow law enforcement people to have access to the proof that they are who they are. Beyond that basis, it would have to be carefully screened—law enforcement, Federal law enforcement basis. But I think if a highway patrolman pulls you over, and this is part of your proof of who you are, it ought to be reasonable for them to have at least the negative access that says, yes, this is a real person.

Mrs. MALONEY. The other panelists?

Mr. MCCOLLUM. I think what—Newt Gingrich is very clear, but I want to amplify it, and that is the key to all of this in identification and certainly in the area of these aliens who are coming here is the proof that they are who are they are. That verification, that is, that the whole idea if you have a biometric and take your fingerprint and put it here, maybe that goes back to some data base where you corroborate and say, "Hey, that is Joe," but I don't think the general public should have access to it. And I don't think that anybody but law enforcement for very specific purposes, probably Immigration Service and key law enforcement people, should have access to the full information, presumably the data on that alien about where they are born, how many times they have been married, that sort of thing.

Mrs. MALONEY. My time is up.

Mr. HORN. I thank the woman from New York, and now the only librarian in the history of Congress, Major Owens, the gentleman from New York, 5 minutes for questioning.

Mr. OWENS. Thank you, Mr. Chairman.

What this distinguished panel seems to agree, that the national identification card will not be a silver bullet. We can put the debate to rest once and for all and focus instead on another problem that I think most of them would agree we have, and that is the problem of monumental mismanagement in our agencies; you know, the kind of mismanagement which allows us to have a worldwide electronic surveillance system where we can pick up all kinds of information, but they didn't have enough Arab translators in the FBI and CIA to deal with the translation of vital information. I could not believe that when I heard it, you know.

Right now we have a recent airplane crash in New York, and it appears that turbulence of a jet that took off just before is probably the cause of the accident that took place. If after all these years of flying and jets we don't know about turbulence and what it might do to an airplane, or, you know, the mismanagement is such that decisionmaking within these vital agencies like the CIA and FBI is off to the point where Aldrich Ames could sit there for 10 years on the payroll of the Soviet Union and Robert Hansen could be on the payroll of the Soviet Union for 14 years, maybe your prestige and influence could be put to work on a crusade to improve the management—technology is excellent and way ahead of our capacity to use it, including INS computers always breaking down, and there is always a problem. If INS maybe had some of the budget of the CIA—$30 billion plus and trying to maintain enough staff—maybe we could—I will conclude and you can comment—maybe such a crusade of people of your caliber would get to the heart of the matter and all these other things would fall into place.

The companies that issue credit cards are very familiar with ways, and you can develop a foolproof card. Even if there's no foolproof card, there's a certain degree of fraud they put up with, but they are pretty much on top of that. And there are various ways of doing it, and some identification cards, consolidation would be very convenient for most of us.

But the real problem, I think, is monumental mismanagement. I think the history of the fall of the American cyber-civilization might be written 1 day, and the cause will be human error. That is what we ought to address.

Mr. MCCOLLUM. One of the greatest frustrations I had in the last couple of years in Congress was the fact—is that over the years I had been one of the those people who was beating up on the CIA and others to get more language speakers of Farsi and Pashto and all those languages that we're now seeing we don't have. And we kept pouring money at it, and they kept reporting to us, and they kept not getting the numbers and telling us they just weren't available.

Mr. OWENS. They had a lot of people who spoke Russian. A lot of good librarians work for the CIA.

Mr. MCCOLLUM. But my point to you, and you know this because you served with me in a number of these capacities, is that you sit there, and you are only as good as the product or the effort of the person who is right in charge at the moment and the vision they have. And the vision in the case of some of these things, including the language issue you are talking about, had to be to go out and be creative and get that language more quickly in place. The same thing is true about the immigration stuff we're talking about here today. That is why we all hope that some of the ideas being batted here today will really be enacted and that Ziglar and others will go out and do it, and we won't be talking about it.

Mr. OWENS. We had a problem with Arab terrorism since the Beirut bombing when President Reagan was President. There have been Arabs—why after all these years don't they have translators who can translate documents from Arabs?

Mr. GINGRICH. Let me just say, in your 5 minutes, you put your finger on the heart of the American challenge in the sense that is what Senator Simpson said when he wished Tom Ridge luck as part of his Christmas present. And it goes to the core of whether we are a comfortable system or we're a serious system. The difference is a comfortable system accepts any innovation that doesn't require it to change. A serious system says, "This is what has to happen." If you watch Jack Welch of General Electric—probably the best modern CEO—he said for GE to be successful it has to go and become X, and that means we are going to change in the following ways, and he drove the changes.

There are three problems: rivalry, bureaucratism and acquiring new capabilities. Rivalry, the CIA doesn't want to share with the FBI, and the FBI doesn't want to share with anybody. I mean, it is an absurdity, and it should be a national scandal that the watch list didn't get through to Logan Airport after 42 days. The one that Senator Simpson mentioned, the Border Patrol and the Customs agents standing next to each other, have different computers. Now, that's just a level of deliberate bureaucratic turf-guarding that shouldn't be tolerable, and that should be shameful.

Second, bureaucratism. I had my staff pull this up the other day. There are 51,000 Pashtuns in the United States. Now, if the Central Intelligence Agency can't find Pashtun speakers, they should assign someone to go to National Airport and wait for the taxis to come in. The idea that you couldn't hire a translator—you don't have to go through the process of vetting somebody to be an FBI agent or vetting them to be a CIA agent with secrets in order to have them as a translator. The notion that you couldn't find an Arab translator in the FBI is that it tells you how bureaucratic they were, how lacking in drive and seriousness, and how unwilling to confront reality.

Third, I mentioned earlier before you got here—as a librarian, you will appreciate that I am pushing books. I mentioned Clayton Christenson's book on, the Innovator's Dilemma, because he really makes the key point. Really big breakthroughs tend to come in really small companies, just the nature of how breakthroughs occur. Government is peculiarly slow at finding those. Government procurement makes it almost guaranteed not to acquire the newest technologies.

And so I think you put your finger on a profound challenge for the American Government. I wish President Bush well and Director Ridge well in trying to get this thing solved, but I think you have absolutely described the core problem of us becoming an effective country in the next decade.

Mr. SIMPSON. May I say a word to my friend Major Owens, who I have enjoyed very much through the years? We have had some nice sessions together and traveled together. You are absolutely correct when you are talking about mismanagement, and then you are talking about the thing that all of us never do well when we are here, and it is called oversight hearings. We have an oversight hearing. We bring in an agency. They prepare for it. Oh, man, do they get ready for it. And then you beat them up. And everybody just beats their brains out from up on the panel. And they all say, don't worry, we recognize that. We are going to correct it. In fact, we are so thrilled that you see, too, this is a problem for us.

So after pounding their brains in all day, and after them slip-sliding along like that old play, the Best Little Whorehouse in Texas, where the guy just slid all over the place, we don't do anything. I couldn't do anything. I had oversight hearings with the INS, and they told me the most magnificent things for 18 years, and nothing was ever done. It was with violin music in the background and tympany and bells. But it is oversight, and that is the tough one.

Mr. HORN. I am going to give you one more question. And in his testimony—for the panel, too—Professor Turley will propose that a commission be established to study the feasibility of a national identification system. What do you think of that proposal? You have been on these commissions. Should they do it, whoever they are, Presidential and leadership in both Chambers, or have legislators go up to the trough and see what they can do?

Mr. SIMPSON. I think that a national commission—I speak from experience. The Select Commission did two reports on legal and illegal immigration, by the chairman, Ted Hesburgh, and both of the commission reports were enacted into law—the essence of the legislation. So I do think it's good. I do think that it has to be—it has to be not called a national identifier. It should be called how to make more secure the systems of identification and work recognition in America, or something like that. If you use national ID, it's over.

Mr. MCCOLLUM. I believe, as Senator Simpson does, that the commissions do form the nucleus and sometimes the initial impetus to get legislation enacted when you need to get a consensus together. And I share his concern. The whole idea of the national ID, as I described it in my statement to you, Mr. Chairman, is a nonstarter, and we don't want to talk about it. Not that we don't want to recognize that people could call something that, but I don't want a national ID with a national data base with Big Brother. But I do want to see improvements that a commission could recommend and make things more secure and an identification that really works in this country.

Mr. GINGRICH. Let me be a doubter for just a second. I'm not opposed to a commission, but I think we know an awful lot of what needs to happen. And the Congress, I think, could move expeditiously early next year on an awful lot of stuff particularly as it relates to non-citizens. We really know how much we have to improve that system, and I am not sure that we need to have more people tell us. I suspect if you had your staff go to the Library of Congress and pull up all the commissions on this topic in the last 20 years and simply print out the summary of recommendations, you'd be astonished how much already exists and how many smart people have already worked the issue. And I think it is important to move while the public is paying attention and cares about this topic, and that would be in the next session of Congress, not 3 years from now.

Mr. MCCOLLUM. And by the way, I'd echo that. I think he's absolutely right about that point.

Mr. HORN. Well, I thank you all for coming. I know when the three of you get together, it's going to be a lively session. So we wish you well. Thank you.

We will go to the second panel now. Mr. Turley, Mr. Goodman, Ms. Corrigan—would you all stand, please, to be sworn.

[Witnesses sworn.]

Mr. HORN. Didn't see too many other assistants. So let us start, then, with Mr. Turley, Shapiro professor of public interest law at the George Washington Law School. Mr. Turley.

STATEMENTS OF JONATHAN TURLEY, SHAPIRO PROFESSOR OF PUBLIC INTEREST LAW, THE GEORGE WASHINGTON UNIVERSITY LAW SCHOOL; ROY M. GOODMAN, CHAIRMAN, INVESTIGATIONS COMMITTEE, NEW YORK STATE SENATE; KATIE CORRIGAN, LEGISLATIVE COUNSEL ON PRIVACY, AMERICAN CIVIL LIBERTIES UNION; RUDI VEESTRAETEN, COUNSELOR AND CONSUL, EMBASSY OF BELGIUM; TIM HOECHST, SENIOR VICE PRESIDENT OF TECHNOLOGY, ORACLE CORP.; AND BEN SHNEIDERMAN, PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF MARYLAND, COLLEGE PARK, FELLOW, ASSOCIATION FOR COMPUTING MACHINERY

Mr. TURLEY. Thank you very much, Mr. Chairman. First of all, let me express my thanks for appearing again before this subcommittee and also to appear before you, perhaps for my last time, as chairman of this subcommittee. We owe you a great debt, and your retirement is a real loss to this institution. I want to be one that thanks you for it.

Mr. HORN. Remember you are under oath now.

Mr. TURLEY. Obviously this is a subject where generally more heat than light is generated. And in a rare display of academic modesty, I will say that I will not resolve the questions surrounding this debate. I would, however, like to offer a Constitutional historical foundation perhaps to move the debate from what is often kinetic rhetoric to a more stable basis for discussion.

It is certainly not enough to dismiss national identification systems as opposed to a card as unprecedented. The framers gave us a system that is—was certainly at the time—unique because it is the most nimble and versatile system in the world. As in nature, nations that fail to evolve are least likely to survive. The world is not static, and so our responses have to be as dynamic as the world around us. So this is a hearing that is looking at a question that is very much a question for our times.

Whether you consider the national identification system to be a necessary security measure or Big Brother's little helper, we need to reach some type of consensus, and so it is an honor to offer my views on those lines. Now, today's debate is part of a long unbroken debate that has raged about the relationship between the government and the governed. We as Americans have a virtual hereditary suspicion of government. As Oliver Wendell Holmes said, “The life of law has not been logic, it's been experience.” And our experience with the government and systems of this kind has not been good. It has been long and painful.

We have learned that government authority operates along the same principles as a gas in a closed space. As you expand that space, government authority will expand as well to the full extent of the expansion. And from Biblical times, and I have laid this out in my written testimony, through the Ottoman Empire and Henry VIII, nations have tried to create national registries not for oppressive reasons, but for necessary reasons, but those systems have, as we know, been used for great harm.

Now, we also need to get away from a habit of talking a good game about national identification systems. We are very proud as Americans that we don't have human license plates. But the fact is we have a national identification system, it just happens to not be a very good one. We have allowed the Social Security number to mutate into a national identifier. That is ironic since, as I mention in my testimony, the Congress was quite clear that the Social Security number was not to be used as a source of identification. This Congress has repeatedly said that it should not be used and that it's opposed to a national identification. And so the question is why in my wallet do I have a driver's license, a smart university card, an athletic card and credit cards that are all based on my SSN? Why do I have two kids, one is 3 and one who is 1½, have their own cards? They're already being tracked.

The human serialization that we fear is here in some respects, but the reason it is here and the reason we failed in our efforts to control the SSN is because the market had a need. It created a vacuum that, in the absence of congressional involvement, it filled that vacuum. The SSN was inevitable because the market needed it.

I happen to have a great deal of problems with national identification systems. I tend to fear government, quite frankly. I tend to like the least of it as I possibly can have. But we also have to be concerned that if we do not act, that the market will act for us. We have to be concerned that if we remain passive, there will be efforts to fill that vacuum, and they are happening right now. At this moment, the heads of the Department of Motor Vehicles have already moved toward what's called a de facto national identification card. The airlines are working on a fast track card of their own that will effectively have a national footprint. Now, I don't know the heads of the Department of Motor Vehicles, quite frankly. Maybe I should. But I don't think they are the ones who should make this decision. I think you are the ones who should make this decision. And it is important for you, I believe, not to be repelled by the idea, to the extent, of being absent.

I happen to believe, and I may disagree with our earlier panel, that we may want to discourage the development of those cards. We may want to try to exercise some degree of control as to what is happening in the country in terms of identifications, if nothing else, to avoid the creation of redundant systems where we suddenly have a whole bunch of cards that become barriers to travel.

In the review of identification cards around the world, you have over 100 nations with different cards, but to use the term "national identification system," let alone "national identification card," is virtually meaningless. These systems are unbelievably diverse. Some of them are really better than our SSN system. Others are incredibly detailed and are attached to data banks and probably would make most Americans feel uneasy. But using the reference to Nazi Germany and to the abuses, I think, is a little bit overblown, but it is relevant. It is overblown in the sense that we have a Nation that has its own safeguards, Constitutional safeguards, cultural safeguards, that makes those types of abuses historical, but not contemporarily relevant. Many of our friends around the world like Belgium, France and Germany are great democracies, and yet they have these cards. So I think we need to look at this with the appropriate amount of passion, but also with an open mind.

Now, the cards differ, of course, dramatically. Britain had a national identification system that was discontinued in the 1950's when they had a negative ruling by the lower Chief Justice. They are now considering a new card, and they range—we can look at, for example, the Belgium identification card, which is one of the most developed of systems. And in Belgium, you are required to have a card at age 12, and then you are required to carry it by age 15. It is not an internal passport system in the most negative sense, but it is a potential barrier in the sense that when you go to an airport in Belgium, you do have to show the card. Obviously Belgium has not used that card for oppressive means. They have a large data base that the police have access to.

Germany also requires the carrying of a card, and it has a great deal of information. It is incorporated into a data base which is accessed from multiple sources, like Belgium it is a stand-alone system. Other countries like, for example, for the Dutch, they have the SoFi number, which is a more developed system than our Social Security system. It is sort of a hybrid between these various options. And you can go through country to country to look at these options.

As we move toward a national identification system, if we are going to move toward that, then we need to look at the Constitutional and legal parameters for that system, because we are all talking about so far a system more of authentication. It seems we are mainly talking about here—and the Members have already indicated they are interested in authenticating people—is to make sure they are the people that they say they are.

So we have to distinguish between what we are trying to achieve. Are we trying to get a ready identification that is reliable for the cop on the beat so he can take a look, and the card has biometrics and other elements that make it hard to tamper with? If that is the case, the card can be largely contentless. It simply requires those biometric elements to be reliable as authentication. If we are talking about, as has been discussed in the past, a Smart Card attached to a data base, we are talking about far more significant issues in terms of Constitutional and legal questions.

One of the most important Constitutional questions that has to be dealt with is the right of travel. The Supreme Court has said that the right of travel is virtually unconditional in the United States. And when we develop national identification systems, we have to be concerned not just in drift, but that those systems can create barriers to travel that will impinge upon that right. And I go into that in my testimony.

We also have to be concerned about creating a national identification system that will fall into the trap of the Brady law. To some extent, any national identification system will require the integration of State and Federal systems. To the extent that we commandeer the State agencies, we are moving into a separate area where Constitutional concerns would be heightened.

And finally, privacy protections, which I talk about in my testimony. What I would like to propose is that Congress consider—one thing that I think is clear, and clarity in this matter is truly valuable. It should not necessarily be clear how we should proceed, but it should be clear how we should not proceed. We need to look at the SSN experience and not repeat it. That's not how we do national policy.

We allowed the SSN to be propelled into a national identifier without any vote of this body. There were a couple of laws in which Congress embraced the SSN. Franklin Delano Roosevelt wanted to use the SSN, but for the most part this has been done with little foresight and control. And as we see these de facto identification cards in the making, it seems that history is repeating itself. So that is the reason I recommended the creation of a Federal commission, and God knows this town does not require another commission. I have been on a Federal advisory group. I was on it for 3 years, and at the end I wanted to take a ball-peen-hammer to my head. They are frustrating. There's too many of them, but, unfortunately, I think this is an area that deserves a commission unlike the ones we have seen in the past.

Newt Gingrich is right. We have had commissions in this area, but none have been given the specific task of looking at whether we are going to have a national identification system. Whether or not we act or not, that is important. We need to have a commission that looks at the question of whether there is inevitability. Whether in this information age we are going to have this Cosean problem where the market is going to dictate those conditions unless you do something.

So we have to deal with reality, and if that reality is that businesses and agencies need a national identifier, I would rather have you involved in it than the hidden hand of a market which may take us away from privacy.

The commission can look at some questions I've laid out in my testimony. The first one is what the function, utility of a national identification card is. I have already mentioned that, but there are vast differences, and when you look at what people have said about national identification systems, they are as different as you can possibly be. Some of them talk about massive data bases, and some of them talk about immediate authentication. I don't know which one we need, but we need to look at that before we do anything.

Second, we have to look at the utility of the system. Part of the problem with a national identification card is that you can have a sleeper agent from Al Qaeda or an espionage agent. In the United States, one of the most effective ways to penetrate a nation is to have a sleeper, and he or she comes into the country. She has a wonderful life, is a wonderful neighbor, goes to PTA meetings, and then about 9 years down the road, Al Qaeda activates her. She's got a wallet for every possible card from the PTA to a fasttrack card to a national identification card.

Finally, we need also—second, we need to look at what technology is to be used for the system. We have everything from iris recognition to DNA fingerprinting to facial recognition systems. We need to look at those technologies. If we are going to embrace the technology, embrace one that is going to be good 10 years from now, that is going to be accurate and reliable.

We need to look at the system of hacking, because if this is going to be a system like Belgium's where you need to get it on a plane, then, frankly, it is dangerous to have the usual Government error rate with data bank and data bases.

Finally, we need to look at what type of protections we need to put in place. As you know, the Census Bureau information is supposed to be private, but it was used to round up Japanese Americans. We know information from States have been sold to private companies.

And then finally, I have suggested that we consider the need for a Constitutional amendment. I have never supported a Constitutional amendment until this year, but there is a trend that needs to be arrested, and that trend is the diminishment of privacy. It's chilling to hear a person like Simpson, who I have a huge amount of respect for, saying privacy is dead, because if privacy is dead, we have allowed something that is uniquely American to die with it.

So in conclusion, the test for the moment is to try to protect our society without changing it in the way that we lose the object of our defense. The Framers never said it would be an easy road, they simply said it was the only road for a free people. And so I suppose the charge of the Framers is this: How to keep us safe from harm, but to pass along our system to the next generation in the condition it was passed to us. I think that is a subject that deserves some thought and circumspection.

I thank you very much for your time today.

Mr. HORN. We thank you very much for your presentation.

[The prepared statement of Mr. Turley follows:]

STATEMENT OF
PROFESSOR JONATHAN TURLEY
SHAPIRO PROFESSOR OF PUBLIC INTEREST LAW
GEORGE WASHINGTON UNIVERSITY LAW SCHOOL
WASHINGTON, D.C.

"OVERSIGHT HEARING ON NATIONAL IDENTIFICATION CARDS"

NOVEMBER 16, 2001

Thank you, Mr. Chairman, it is an honor to appear again before this Committee and its distinguished members. I am particularly grateful for the opportunity to appear for what may be the last time before you, Chairman Horn, before your retirement. From your first public service with the Eisenhower Administration to your work as a congressional staffer on major legislation like the Civil Rights Act of 1964 to your leadership of this Subcommittee, you have been widely viewed as a voice of moderation and experience in government. We all owe you, and your wife Nini, a great debt for the commitment and contribution that you have made to public service.

I. INTRODUCTION

Chairman Horn, Vice-Chairman Lewis, Ranking Member Schakowsky, members of the Subcommittee, my name is Jonathan Turley and I am a law professor at the George Washington University Law School where I hold the J.B. and Maurice C. Shapiro Chair for Public Interest Law.[1] I know that your time is limited today and, with the consent of the Subcommittee, I would like to submit a longer written statement to augment my oral testimony.

The creation of a national identification card or tracking system is a subject that tends to polarize discussions. There has certainly been more heat than light in the recent debate after our national tragedy on September 11th. In a rare display of academic modesty, I will not even suggest that I have the answer to this debate. I would like, however, to try to lay the foundation historically and legally for this question. I would then like to suggest a modest proposal on how I believe the government could best proceed in this area. If nothing else, I would like to dispel some common misconceptions on both sides of this debate. Perhaps if we can better isolate

[1] I come to this question with both professional and academic interests. I teach constitutional and tort subjects at George Washington Law School. My academic writings include work on a variety of relevant areas, including past publications on national security law, constitutional law, surveillance law, and even military law. I have also worked and litigated in the areas of constitutional and national security law, including the recent Daniel King espionage case. I have no connection with any of the companies with financial interests in the development of either national identification systems or new secure travel technology. Likewise, while I once worked at the National Security Agency (NSA), I have no consulting or contract relationship with any governmental agency at this time.

the live components of this problem, we may find some ground for reasoned compromise.

The instinctual resistance to any national identification system is understandable but often misplaced. We already have a national identification system and the only question is whether we should create a more integrated and uniform system. It is not enough to simply reject such proposals as "unprecedented." It is important to remember that the Framers gave us a constitutional system that is the most nimble in the world. Whether acting to maximize profits or protection for our citizens, it is a system that is unparalleled in its ability to respond and adjust to new realities. As in nature, nations which fail to evolve are the least likely to survive and flourish. We should not be fearful or hostile to new ideas on how to better protect our citizens against new threats. The world is not static and our national policies must be as dynamic as the conditions under which we live.

Nevertheless, we have come this far due to the liberties that define our nation, not in spite of those liberties. There are troubling aspects to national identification systems that deserve considerable caution from Congress. Unfortunately, in the area of national identity systems and databases, we have allowed our national policies to be controlled by events. We have lacked any coherent, forward-looking approach. If nothing else, the current debate should be a catalyst for such a serious review of the existing tracking systems, databases, and authentication systems. Whether one views a national identification card as a necessary security measure or Big Brother's little helper, it is a subject on which the United States must reach some consensus. It is an honor to offer my own views on where such a consensus might be forged.

I have five basic conclusions or proposals to offer today.

First, our historical experience with a quasi-national identification number (the social security number) warrants the attention of Congress. Regardless of the outcome, we should strive to avoid the same mistakes of omission and acquiescence. If we are to have a national identification system, Congress and not the market should shape and maintain it. Moreover, the current effort of the heads of Departments of Motor Vehicles to create a "de facto national identification card" should be discouraged in favor of a deliberative decision of Congress.

Second, a national identification card would be constitutional as a general matter, though complications can arise as the details of program emerge. Moreover, analogies to notorious internal passport systems like the Nazi citizen papers are often over-blown given constitutional and cultural realities in the United States. There are, however, a number of constitutional and legal issues that would have to be addressed before any program is rolled out.

Third, a review of different national identification systems worldwide reveals considerable differences and variations. Some of these systems (as will be shown below) have mandatory elements that would run against the American grain while other systems achieve little more than a variation on the use of the social security number as a national registry or identifier.

Fourth, there is a compelling basis to attempt to establish a uniform identification card with biometric elements[2] for certain insular groups regardless of whether a national identification card is later embraced and designed. Such groups may include foreign nationals residing in the country, certain categories of truckers (such a hazardous waste haulers and international truckers), researchers with access to such material as anthrax,

[2] A biometric is defined as " a measurable physical characteristic or personal trait used to recognize the identity, or verify the claimed identity, of a person through automated means." "The Use of Social Security Number as a National Identifier," Hearings Before the Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 1st Sess. 58 (1991).

and other high-risk areas. Given our experience with the social security number, however, we need to consider legislation that would prevent "drift" in the use of such a card.

Fifth, and finally, I believe that the most responsible course of action is for Congress to establish a commission to study both the need and function of a national identification card. I have set out a number of issues that would be relevant to such an inquiry, including the possible need for new privacy protections. Such protections might include the need for constitutional amendment that would not only protect against the abuses of a national identification system but arrest a disturbing trend of diminishing privacy expectations in the country.

II. HISTORICAL BACKGROUND

A. The American Historical and Cultural Opposition to Governmental Intrusion and Surveillance.

While today's hearing addresses the subject of a national identity system, it is part of a debate that has raged since our founding over the uneasy relationship between the government and the governed.

It is fair to say that Americans have an almost hereditary suspicion of government. While there has been some change with the expanded role of the federal government after World War II (and especially the Great Society period), there remains a lingering mistrust of expanding governmental authority and enforcement capabilities. This view has been reinforced by the government, which has carried out periodic abuses in the nineteenth and twentieth centuries.[3] This history must necessarily inform our actions today if history is not to repeat itself. As Oliver Wendell Holmes once said, "the life of the law has not been logic; it has been experience."[4] Our experience with the expansion of governmental authority has been marked by many painful periods ranging from the Palmer Raids to the Japanese Internment to the Red Scare to the more recent intelligence scandals of the 1960s and 1970s. Such expansion and attending abuses often occur at times of emergency where Congress and the public relax their guard and their vigilance. We have learned from experience that governmental power operates on the same principles as a gas in a closed space. As a confined space is increased, both a gas and governmental power will expand to fill the full extent of the available space.

[3] Veronica Sch. Dist. 47J v. Acton, 515 U.S. 646, 686 (1995) (O'Connor, J., dissenting) (""The greatest threats to our constitutional freedoms come in times of crisis.").

[4] O. W. HOLMES, THE COMMON LAW 1 (1881).

The American resistance to governmental surveillance and monitoring may be stronger than any other country due to both our history and geography. Obviously, we are a nation founded by people who largely fled other governments. They created a constitutional system on the premise articulated by James Madison that "[i]n framing a government which is to be administered by men over men, the great difficulty lics in this: you must first enable the government to control the governed; and in the next place oblige it to control itself."[5] While not all Framers took as dim a view of human nature as William Lenoir who insisted that all men were beasts driven to tyranny,[6] most insisted that the safest way to govern and to legislate was to consider any proposed power in the hands of individuals with the worst motivations or inclinations in government.[7] For this reason, Madison and

[5] THE FEDERALIST No. 51, at 322 (J. Madison) (C. Rossiter ed., 1961).

[6] William Lenoir, Address to the North Carolina Ratifying Convention (July 30, 1788) ("It is the nature of mankind to be tyrannical. . . . We ought to consider the depravity of human nature [and] the predominant thirst of power which is in the breast of every one.").

[7] This view was summed up by Madison's famous observation that "[i]f angels were to govern men, neither external nor internal controls on government would be necessary." THE FEDERALIST No. 51, at 322 (J. Madison) (C. Rossiter ed., 1961); see also William Grayson, Address to the Virginia Ratifying Convention (June 21, 1788) ("Power . . . ought to be granted on a supposition that men will be bad.")).

others crafted a system with not the best, but the worst, human qualities in mind.

One other important element to our historical resistance to governmental authority was our geography and topography. Unlike many European nations that had largely fixed borders, the United States developed with a strong frontier mentality. It was easy to remove oneself from virtually any interaction with the government by simply moving West. This huge expanse also made it difficult for the government to attempt anything more than rudimentary governing tasks in much of the nation. The size of the territory and limited technology simply made tyrannical measures impractical, even if they were attempted.[8] Even when the United States reached its physical limitation on territory, the size of our population placed other practical barriers to the government in any widespread abuses of surveillance.[9] Our greatest protections in this sense may not have been our

[8] This did not prevent periodic measures that could be viewed as tyrannical such as the Alien and Sedition Act prosecutions under President John Adams.

[9] These practical barriers were recognized by Congress in prior privacy hearings going back decades. In 1966, for example, Rep. Frank Norton noted that "[o]ne of the most practical of our present safeguards of privacy is the fragmented nature of personal information. It is scattered in little bits across the geography and years of our life." "The Computer and the Invasion of Privacy," Hearings before the Special Subcommittee, on

traditions but the sheer costs and difficulties of monitoring the population. As will be shown, we are now beginning a new chapter of our history with the evolution of technology that, for the first time, has overcome the practical barriers of population size and territorial expanse. Moreover, powerful market forces continue to spur the development and deployment of such technologies and databases. There may be a Coasean inevitability[10] to this trend regardless of legislative measures. The question may be less whether a more integrated national identification system is developed but who will dictate the features and uses of that system.

B. The American with National Identification and Tracking Systems.

Systems that monitor, track or control the movement of citizens have been common in many areas of the world for centuries. The Ottoman Empire and other former regimes were known to keep extensive dossiers and

Invasion of Privacy, Committee on Government Operations, U.S. House of Representatives, 89th Cong., 2nd Sess. 6 (1966).

[10] Ronald H. Coase, The Problem of Social Cost, 3 J.L. & Econ. 1 (1960). On its most basic level, the Coase Theorem suggests that, in a perfect market, the market and not the law will control the outcome of conflicts in resources and activities. By analogy, one can see a conflict between privacy and efficiency that will be heavily influenced, if not resolved, by powerful market forces. For example, the airlines are considering the creation of a "fast-card" system in which citizens would subject themselves to background checks in return for more expedited

intelligence information on significant numbers of citizens. The single most important component of such a system is the ability to catalogue and cross-reference files on citizens. Even if a government has files on every citizen, such information is only useful as a tool of oppression if it can be accessed easily and reliably. The importance of national identifiers to such system was not lost on Americans. Americans have historically expressed strong opposition to a national identification system for civic, practical, and even religious reasons.[11] This resistance grew in intensity after World War II when the use of internal passports by the Germans allowed for unprecedented control over a large European society and was a critical asset used by the Nazi's to carry out their genocidal crimes against Jews, Gypsies, and other races.

For all intents and purposes, the United States already has a system of national identification and database systems of personal information on virtually every citizen. The evolution of the Social Security Number (SSN)

treatment at security check points. In such insular trade-offs, it is likely that privacy concerns will lose to incremental benefits in the market.

[11] The most bizarre expression of this opposition has been the connection of national identification system to Revelation 13:4 and the coming of the apocalypse. Revelation 13:4 ("[The false prophet] forced everyone, small and great, rich and poor, free and slave, to receive a mark on his right hand or on this forehead, so that no one could buy or sell unless he had the mark, which is the name of the beast or the number of his name.")

as a national identifier is worthy of close consideration by Congress as part of any renewed interest in a new national identification system. The SSN was not the product of legislation but regulation. The Social Security Act of 1935[12] did not contain any express authorization for the numbering of all citizens. Rather, a number was quickly embraced by the government as a "reasonable device or method[]" to carry out the objectives of the Act. After the government began to utilize a national number identifier for social security, various members of Congress grew uneasy with the implications of such a system. Congress barred the use of the number as a form of identification to forestall the creation of a single national identification or tracking system.[13]

[12] Social Security Act, ch. 531, 49 Stat. 620 (1935).

[13] Social security cards used have the following statement on every card: "This card is not to be used for identification." See generally "The Use of Social Security Number as a National Identifier," Hearings Before the Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 1st Sess. (1991). The late Barry Goldwater often spoke against the expanded use of the SSN as a threat to liberty and part of a "drift toward reducing each person to a number." "The National ID Card: Big Government at its Worst or Technological Efficiency?" Hearings Before the Subcommittee on National Economic Growth, National Resources, and Regulatory Affairs, Committee on Government Reform and Oversight, U.S. House of Representatives, 2d Sess., 22 (1998). Congress has been of two minds on this subject. It has expressly rejected proposals that would have banned the use of the SSN as a national identifier. See, e.g., S. REP. NO. 1183, 93d Cong., 2d Sess. 4 (1974), *reprinted in* 1974 U.S.C.C.A.N. 6916,

By 1943, President Franklin Delano Roosevelt had issued an executive order that sought to further establish the social security number as a single system of identification for the government. Ultimately, three agencies established the first formal uses of the number as a national identifier: the Civil Service Commission in 1961; the Internal Revenue System in 1962; and the Department of Defense in 1967.[14] Not long after, the social security number was legislatively mandated by Congress as an identifier for federal benefits recipients ranging from Medicaid to food stamps to federal loans. Legal aliens were also required to be identified with use of SSNs.[15] As the federal use of the SSN increased, the states also began to mandate the use of this national identifier with some states like Virginia making drivers license numbers the same as an individual's SSN. Today, by congressional mandate,[16] all children above the age of one must receive a SSN from the government and citizens routinely repeat their number for a wide variety of government and private transactions as their identity.

6943-46. Yet, it has also opposed the creation of a national identification card. See, e.g., 8 U.S.C. §1324(c) (1988).

[14] See generally William H. Minor, Identity Cards and Databases in Health Care: The Need for Federal Privacy Protections, 28 Colum. J.L. & Soc. Probs. 253 (1995).

[15] Social Security Amendments of 1972; 42 U.S.C. §§405 (c) (2) (B)(i).

[16] Omnibus Budget Reconciliation Act of 1990, Pub. L. No. 101-508, § 1112(a), 104 Stat. 1388, 1388-413 (1990); 26 U.S.C. §6109(e) (1990).

Anyone in this room can be a witness to the comprehensive use of national tracking systems and databases keyed into the social security number. For example, in my wallet is a (1) driver's license; (2) university identification "smart" card; (3) voter's registration card; (4) insurance card; (5) credit cards; and (6) even a pool pass that have either my SSN number on the front or are based on the SSN as my personal tracking code. My two sons – ages three and one-and-a-half – are already being tracked in this system. Benjamin and Jack have their own social security cards, giving them their individual numerical identifications that they will carry through life. They have been serialized as citizens in a national tracking system that is both disturbing and understandable.

In the United States, as well as other countries like Australia and New Zealand,[17] there have been public backlashes to such national identification systems.[18] Despite the exponential growth in use of the SSN as a national identifier, this opposition remained strong until some diminishment after the

[17] In 1987, the "Australia Card" was abandoned in the face of public opposition. In 1991, similar opposition successfully defeated the "Kiwi Card" in New Zealand.

[18] Only a few years ago, the proposal of then Senator Alan Simpson were denounced by other members as "instruments of a police state." Ann Davis, Digital IDs For Workers in the Cards, The National Law Journal, April 10, 1995.

attacks.[19] Congress has debated the implementation of a national identification card on an almost annual basis in areas like immigration and health care. While the Congress has come close on some occasions to the creation of such a system for select populations like immigrants, there has always been sufficient disagreement in one house or in conference to forestall implementation.[20] In 1976, the idea of such a system was sufficiently repugnant to members that Congress added the following language to the Immigration Reform and Control Act of 1976: "Nothing in this section shall be construed to authorize directly or indirectly, the issuance or use of a national identification card or the establishment of a national identification card."[21] Similarly, President Clinton's attempt to create a national health care card was opposed by Rep. Dick Armey and others who

[19] See The Use of Social Security Number as a National Identifier," Hearings Before the Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, 102nd Cong. 1st Sess. 121 (1991) (discussing government studies that found widespread opposition to the use of the SSN as a national identifier.").

[20] In 1973, the Advisory Committee to the United States Department of Health, Education, and Welfare formally recommended against any "standard universal identifier" be used in the United States. the United States Department of Health, Education, and Welfare, Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems 122 (1973).

[21] 8 U.S.C. §1324(c) (1988).

oppose any move toward a national identification card.[22] However, in a sharp departure from earlier polls, recent polls show that Americans (at least temporarily) have swung heavily in favor of such cards after the terrorist attacks.[23]

C. International Identification Systems and the Need for Greater Distinctions Between Types of Identification, Authentication, and Tracking Systems.

Stretching back to the biblical censuses, governments have long struggled to maintain records on the number and identity of individuals within their borders. One of the early crude "database" efforts can be traced to Henry VIII decree in 1538 requiring parish priests to keep registers of births, deaths and marriages in England. Various governments not only struggled to create such lists but there were also various crude forms of

[22] Minor, supra, at 273 (quoting public statement of Rep. Armey that "[w]e didn't beat back the administration's plan to issue us all 'health security cards' only to have Congress adopt an I.D. card to track down immigrants.")

[23] Mike Dorning, Travelers May Shed Privacy to Speed Screening, Chicago Tribune, November 9, 2001, at 1 (noting recent Pew Research Center poll finding that seventy percent favoring a mandatory national identification card). Ironically, the seventy percent of polled citizens who favor such a card is the same percentage that earlier opposed such systems. See Robert S. Peck, Extending the Constitutional Right to Privacy in the New Technological Age, 12 Hofstra L. Rev. 893, 894 (1984) (detailing polls showing the seventy percent of polled individuals believed that the government would use private information to intimidate citizens).

personal identity that were widely used for class and cultural reasons.[24] In the 1700s, rudimentary internal passports were used in some European countries for any travel of citizens within their borders.[25] With time, however, the interest of governments in authentication and control required more detailed and sophisticated systems of identification.

The lasting influence of our experience in World War II is no more evident than in the area of national identification cards. The familiar bark of "your papers, please!" by German *Gestapo* was seared in the minds of Americans and reinforced later by the abuses of Communist internal security systems. It is important, however, to distinguish between types of identity systems. The Nazis employed an internal passport that controlled and tracked the movement of citizens. It was used also to identify religious and ethnic minority status, such as the infamous "J" for "*Juden*" on the papers of

[24] National programs of identification are quite old, though the reasons for such tracking has changed. Earlier forms of identification were often done through actual marking, tattooing, or branding of individuals to show ownership or social class. Other forms of early identification involved socially enforced dress and appearance codes. Such identification systems were meant not to convey detailed information but readily identifiable class or social information. After the seventeenth century, more tailored or detailed identification systems were devised for actual tracking or demographic needs.

[25] Minor, supra, at 258-59.

German Jews.[26] These papers had to be carried at all times, reinforcing the German view of travel as a privilege rather than a right during World War II. Likewise, Communist nations routinely used internal passports or papers to monitor and control their population.[27]

Analogies to these notorious types of systems in the current debate are relevant but they can be easily overblown. There are constitutional protections in the United States that prevent the Congress or the President from implementing an internal passport system to control travel of our citizens within our borders. Moreover, Western nations like Germany, France, Spain, and Belgium have a variety of national identification cards while maintaining free and democratic systems. While some of these systems would be anathema in the United States, a national identification card is not synonymous with authoritarianism. If there is to be any resolution of this controversy, there must be more specification as to the function and scope of any national identification system.

Among the over 100 countries that employ some form of national identification system, there is considerable variation in their function,

[26] For a picture of the Nazi identification card for Jewish citizens, see THE BLACK BOOK 98 (1946) (The Jewish Black Book Committee).

[27] The Soviet Union used from internal passports and housing registration (*propiska*) to control movement of citizens.

content, and underlying technology. France's *Carte d'Identite Nacionale* is vastly different from Spain's *Documento Nacional de Identidad*.[28] While they serve common functions, dozens of countries ranging from Argentina[29] to Holland to Kenya[30] to Zambia[31] have crafted their national identification system to meet insular needs or concerns. Other nations like Britain have previously abandoned prior national identification card systems out of

[28] The Spanish require citizens to have a *Documento Nacional de Identidad* or the DNI. The DNI is mandatory for all citizens above the age of 14 and are needed for a host of governmental benefits and programs. Spain also requires a separate identification card for health care benefits. Foreigners are given a different identification designation called the *Numero Identification Extranjeros* that is mandatory of any foreigners living in the country. The NIE is generally necessary for activities ranging from establishing telephone and electricity services to establishing any employment.

[29] All citizens in Argentina are required to obtain a national identification card when they are eight-years-old. A second registration occurs after the child reaches seventeen years. Fines are imposed for the failure to register. Argentina enlisted Raytheon E-Systems to develop a tamper-resistant card.

[30] Kenya administers a strict national identification card system in which the card is required for a wide variety of activities ranging from marriages to employment to voting. Kenyans are required to carry the identification with them at all times and there have been complaints over the use of the card as a barrier to voting for some citizens.

[31] In Zambia, all citizens must obtain a green "national registration card" by age sixteen. Citizens are not required to carry the card but they are expected to memorize the number. This is a two-sided paper card. On the front of the card, there is a picture, signature of the registrar, the citizen's signature, and thumb print. On the back of the card, there is the full name of the citizen, the relevant district of residence, special markings, registration date, and card number.

concern over their abuse. Britain maintained a national identification card from 1939 to 1952. Created primarily as part of the national rationing program, the identification card was also used for internal security checks and authentication. In 1952, after an adverse court decision by the Acting Lord Chief Justice, the card was discontinued. The implementation of a new identification card is now under study in England.[32] This new system would be voluntary and would serve as both a driving license and national identification.

Conversely, Belgium has embraced a fully mandatory card (*carte d'identite/identiteitskaart*) that would likely raise insurmountable opposition in the United States. Belgium requires all citizens over the age of fifteen to register and to carry their cards at all time. As in Germany, there is also a registration system for all citizens and residents to record any change in their addresses within eight days. Citizens also must maintain a good citizenship record document (*Certificat de Bonne Vie et Moeurs/Bewijs van Goed Gedrag en Zeden*) that is required for most official documents or transactions.

[32] British citizens appears generally in agreement with American citizens on this issue. Recent polls show roughly 85% supporting the implementation of national identification cards in the wake of the September 11th attacks.

Under German law,[33] all citizens over the age of 16 must have a national identification card, the *Personalausweis*.[34] The *Personalausweis* is machine readable and contains much of the information on a standard passport. The Germans are also required to carry the *Personalausweis*. However, like many European countries, the Germans have collateral tracking systems. For example, within a few days of moving to a new location (even in the same building), citizens must deregister (*Abmeldung*) from the former location and register (*Anmeldung*) at the new location. These registration offices (*Einwohnermeldeamt)* then input such movements into databases.

Other countries put greater emphasis on the use of universal identity number than the actual identification card.[35] Dutch citizens (and permitted residents) are given a social-fiscal number, the "SoFi," that is used for both taxation and identification purposes. This information is computerized and maintained by the National Revenue Service (*Rijksbelastingdienst*). This does not mean that citizens are not tracked to the same degree as a country like Belgium. Actually, in some countries, the most significant tracking

[33] *Gesetz uber Personalauswiese,* BGB1. I.S. 548 §1.

[34] The card is valid for 10 years. A separate card is used for individual sixteen years and younger. This card is valid for only 5 years.

systems are found in collateral documents, which use the universal identification number. The Dutch, for example, impose a variety of collateral permits and registrations that allow for a higher degree of monitoring than in the United States.[36]

There are also radical differences in the content and technology of these national identification systems. For example, in Honduras, national identification has the individual's photograph, basic information, digital fingerprint, and seal of the National Registry of Persons. In Korea, the "National Registration Card" has basic personal information, military record, photograph, two thumbs prints, and an individual's national identification number. On the high end there are countries like Pakistan, which require an identification card with a great variety of personal information ranging from a national identification number to identification marks to parental information. Likewise, there are considerable differences in the mandatory aspects of these systems. French citizens are not required to carry the *Carte d'Identite Nacional* while citizens in Brazil and Belgium are required to carry their national identification at all times.

[35] Other nations like the Democratic Republic of Congo has a card ("*carte d' identite*") but it is not mandatory for citizens.

It is the differences in these systems that should strongly counsel against any attempt to simply roll-out a new card on an expedited basis. As suggested below, there are considerable questions that should be addressed before any effort to implement such a program. Of course, among the issues that should be addressed is whether we truly require a centralized or government-maintained system. This is not a decision that should be made in the fog and frenzy of terrorist attacks. We may need such a system but both the need and the uses of the system warrant the greatest circumspection.

III.
CONSTITUTIONAL AND LEGAL ISSUES

The imposition of a national identification card would not violate the United States Constitution. Congress can require every citizen to participate in a national registry and to acquire both a number and a card as part of that registration. Any constitutional or legal problems would arise in the details of how such a card is used and how such a system is maintained. Unfortunately, there are few details on the scope, function, and means for a national identification system in the United States. It is, therefore, impossible to give concrete assessments of the constitutional or legal

[36] This includes foreigners who are required to register with the "Foreign police" in their district and obtain a residence permit (which must be renewed annually).

barriers to such a system. As a general matter, however, it would not be difficult to design a system that would pass constitutional muster.

One moderating element of any national identification system can be found in the Constitution. In countries like South Africa, the courts viewed travel and access to a travel passport as a privilege and not a right. We have a different tradition,[37] though there are some disturbing challenges articulated to this view in the aftermath of the attacks. The United States has long recognized the right to travel as a constitutional right.[38] The Court has stated that "the nature of our Federal Union and our constitutional concepts of personal liberty unite to require that all citizens be free to travel throughout the length and breadth of our land uninhibited by statutes, rules, or regulations which unreasonably burden or restrict this movement."[39] In Saenz v. Roe, the Supreme Court emphasized that the right to travel is a "virtually unconditional personal right" under our Constitution.[40] Nevertheless, the United States can impose security safeguards on travel.

[37] Notably, however, the United States government did use passports to unconstitutionally deny travel to members of the Communist party under the auspices of the Internal Security Act of 1950. See Aptheker v. Secretary of State, 378 U.S. 500 (1964).

[38] See, e.g., Saenz v. Roe, 526 U.S. 489 (1999); Zobel v. Williams, 457 U.S. 55 (1982); Shapiro v. Thompson, 394 U.S. 618 (1969).

[39] Shapiro, 394 U.S. at 630-31.

[40] 526 U.S. 489 (1999).

The most obvious are licensing, training, and conduct restrictions operators of aircraft, trucks, trains, and other interstate vehicles. Likewise, the Congress can impose conduct restrictions on passengers, including criminal liability for unruly passengers and actions that frustrate security measures. The question is one of degree. Clearly, Congress could require a single national identification card for certain groups like interstate truckers, pilots etc. Likewise, Congress could mandate the use of single national identification number for basic regulatory, permitting, and licensing activities as is common in other countries. The question becomes more interesting when Congress moves into the area of mandatory possession as is the case in Belgium and Brazil. The Supreme Court has never addressed such a restriction and, as a case of first impression, it may prove too intrusive or analogous to an internal passport system for the Court. Of course, the mere establishment of a national identification card would allow private companies to effectively impose this restriction as a necessary form of identification. Nevertheless, adding new barriers to travel will implicate a fundamental right that the Court has repeatedly protected against even indirect limitations.[41]

[41] The Court recognized that the right to travel for every American is as central "as the choice of what he eats, or wears, or reads." Kent v. Dulles,

A second constitutional danger can be found in the implementation of any national identification system. To the extent that this federal program is carried out by the states, it raises different constitutional problems. As the Supreme Court has emphasized in its review of statutes like the Brady Handgun Violence Prevention Act,[42] the federal government cannot commandeer state officers to carry out federal programs.[43] There may not be a need for a significant administrative role for states in such a program, a question that would become more clear as details emerge on the scope of the program. Not only could the federal government fund the necessary administration of a system, but many states would likely readily embrace a more reliable and integrated system as they have the use of the social security number.

Any national identification system would certainly require legislation to modify existing programs utilizing the SSN as a universal system. Such changes could be made through an omnibus statute that would authorize agencies to incorporate the new systems as part of their regulations. It would be likely that the specific agency application of this system would

357 U.S. 116, 126 (1958).

[42] 18 U.S.C. 922, 925A (Supp. V 1993).

[43] See, e.g., Printz v. United States, 521 U.S. 898 (1997); New York v. United States, 505 U.S. 144 (1992).

generate considerable litigation and result in subsequent legislative measures. However, the legal elements to such a system would not be difficult to establish for the initial roll-out of a program. Once again, the scope of necessary legislation would depend on the specifics of the program, an issue addressed more fully below.

IV.
A PROPOSAL FOR CONGRESSIONAL ACTION

In my view, the one element of clarity in this debate should be less how we should proceed than how we should not proceed in addressing this issue. As noted earlier, the ubiquitous use of the SSN by agencies and states came about in a largely unplanned and even unintended fashion. While Congress initially opposed the use of the SSN as a means of identification outside of the social security system, it gradually filled a vacuum within the emerging information revolution. We are now facing the danger of similar development of universal identification cards that could emerge without deliberative debate and consensus. At this moment, Departments of Motor Vehicles are moving toward a "*de facto* national identification card."[44] On another front, airlines are considering a separate identification card to allow passengers to move more swiftly through security. The Air Transport

Association has announced support in the airline industry for a "trusted traveler" card that would require a background check and national registry.[45]

These developments suggest that there is a danger of history repeating itself. Once again, we may be facing new realities that will create a new resource with or without congressional involvement. Our use of the social security number as a form of national identification is an example of how society and market will fill a vacuum left by Congress. As commerce and travel increased exponentially after World War II, the need for some form of consistent identification became acute for both businesses and government agencies. By not addressing that need, the government made the use of the social security number a virtual inevitability.

There is an increasing need for a more reliable form of identification. If Congress again remains passive, the market and governmental agencies will respond in their own way to this need. This is the wrong way and the wrong officials to make such fundamental decisions. Whatever the qualifications of the heads of our respective Departments of Motor Vehicles, no one would suggest that they are the proper or competent officers to

[44] Robert O'Harrow Jr., States Devising Plan for High-Tech National Identification Cards, The Washington Post, November 3, 2001, at A10.

[45] Ricardo Alonso-Zaldivar & Richard Simon, Screening, Travel Ids Sought for Air Safety, Los Angeles Times, November 9, 2001, at A1.

unilaterally craft such a new system. Moreover, absent federal intervention or possibly federal preemption, we risk the development of multiple and redundant systems with attending databanks. This would achieve the very danger that civil libertarians fear: the consolidation of personal information and the development of barriers to movement. Congress should discourage the creation of these ad hoc systems in the interests of both privacy and efficiency. Instead, I recommend the creation of a federal commission with a mandate to study this issue and return a comprehensive report with recommendations.

The creation of a commission on potential national identification and tracking systems could address the full panoply of privacy and security concerns. The commission could also better define and refine the many suggestions relating to a national identification system. The three most significant questions, in my view, are briefly described below.

1. *What is the function or utility of a national identification card or system?*

One of the strangest aspects about the current debate is that the subject appears undefined and fluid. Some individuals refer to the new system as necessary to allow law enforcement to quickly and reliably identify someone in areas like airports and borders. Others refer to a multi-use "smart" card that could be used for an assortment of official and personal tasks with a supporting database. Such a card has previously been considered as part of health care, welfare, and immigration reforms. There is a considerable difference between such functions. If the card is viewed as primarily a means for reliable and fast authentication of an identity, the card can rely on biometric components and would not require significant content or database support. If the national identification card is merely the physical manifestation of a larger tracking and information system, it requires a far greater logistical and legal effort.

Moreover, in considering the utility of a national identification system, we need to look at the true potential as an anti-terrorism measure. It is clear that a national identification could harass and even frustrate a terrorist who enters the country for an attack in the short-term. However, if an organization like the Al-Queda plants a "sleeper" agent in the country, the individual would be able to acquire such a card and benefit from any expedited treatment that it would afford at places like airports. It seems likely that terrorist organizations will learn the same lesson as espionage organizations that the most effective agent is someone who enters a country and remains dormant until activated shortly before an attack or intelligence operation. We need a solid appraisal of whether an identification would offer greater security or merely the appearance of such security.[46] The potential cost to privacy and the perceived freedom of citizens is too high to adopt these systems merely to satisfy a natural desire to "do something" in the face of a new threat.

In exploring the function of such a system, a Commission should also explore the degree to which market and international forces are already moving toward independent systems. We may have to accept that this type of national identification is an inevitable result of our information age. In such a case, it may not be practical to try to get this cat to walk backwards. Instead, we may have to look at ways that the government can direct and control such systems through legislation and preemption. By better understanding the market and governmental pressures, we can better gauge the most compelling needs and options for future individual identification systems. We can offer to gauge the consumer pressures for integrated, multi-purpose identification systems. Many citizens chaff at the need to carry a variety of identifications. This resistance is likely to increase with

[46] Polls have shown a new eagerness of citizens to be subject to an array of new search technologies. See Mike Snider, Technology Offers a Feeling of Security, USA Today, November 15, 2001, at 1D.

the possible implementation of insular industry identifications, like the suggested "fasttrack" or "trusted traveler" airline identification card.

2. *What technology should be the foundation for a new system?*

There are various technological systems that might be used individually or in combination. Current technology allows for a wide range of biometric authentication systems and physical recognition systems. These include iris recognition, hand vein mapping, signature recognition,[47] fingerprint imaging, voice recognition, retinal scans,[48] DNA fingerprinting, and facial recognition systems.[49] Some countries like Germany have cards that are machine readable and other countries are moving to individual barcodes. One of the greatest concerns with a national identification card is also its reliability. There is a well-known error rate among government databases at the Internal Revenue Service, Social Security Administration, and other agencies. If a new national identification card is utilized, it may pose a significant barrier for citizens if there are periodic problems in its

[47] One such system was employed by the Netherlands to identify methadone addicts. The system tracks how a person signs a document by measuring speed and pen pressure as well as the signature itself.

[48] Retinal scans record blood vessels in the retina as opposed to iris scans.

[49] Current facial-recognition technology such as Facematcher allows for databases that can check a thousand images per minute after an individual image has been captured.

supporting databases or computer systems. If such a system has an alert or caution warning, a citizen could be effectively prevented from long-distance travel by bureaucratic snafus. Accordingly, if the card is used to track and, in some cases, restrain movement, the issue of errors and glitches become extremely important. Finally, different technological options will have bearing on the security of both the card from tampering and the security of databases from hacking. One of the most pressing dangers will be the over-reliance on a system that could result in widespread shutdowns due to either technical problems or tampering.

3. *What structural and legal protections can be enacted in conjunction with such a system to address privacy and civil liberty concerns?*

Any national identification system would require clear and immutable protections from abuse. Past assurances of the government in the use of such databases have often been honored only in the breach by both the federal and state governments. The federal government used confidential Census Bureau information to round up Japanese-Americans for internment in World War II.[50] Likewise, states have sold driver's license information to

[50] The Nazi regime used similar records in the Netherlands to round up Jews and other citizens in countries like the Netherlands, which had maintained comprehensive national registries.

private industry.[51] Finally, as shown by the recent IRS hearings, individual federal employees have violated the privacy of individuals by reviewing government filings or databases.[52] A national identification system increases the potential harm from such "cases of authorized misuse."

In crafting these protective components of any national identification system, it is important to reaffirm and protect the right to travel. While clearly the government can and should restrict travel of criminal actors or suspected terrorists, it is important to resist the erosion of this right. Travel, including air travel, should never be allowed to become a discretionary privilege dependent on "good-standing" with the government. One protection of this right would be the enactment of strong citizen suit provisions to allow for "private attorneys general" to police the conduct of both the government and industry.

Finally, we should consider the need not just for legislation but an actual constitutional amendment concerning privacy. The greatest guarantee of the rights of citizens would be to articulate a comprehensive constitutional amendment that finally deals with the many modern threats to individual

[51] See generally Reno v. Condon, 528 U.S. 141 (2000).

[52] "IRS Oversight," Hearing Before the Senate Finance Committee, U.S. Senate, 105th Cong. 2nd Sess. (1998); see generally Crunchtime for the IRS,

privacy. While I have opposed virtually every proposed constitutional amendment in the last decade, privacy is an area where the Constitution has always been uncomfortably ambiguous. We live at a time when threats to privacy are emerging from innumerable sources. If we are to arrest this trend, it may require our ultimate statement as a free people in the form of a constitutional amendment.

V.
CONCLUSION

As a nation, we have long resisted efforts that would create a "human license plate" that would track and potentially restrict our movement in society. Faced with an onslaught of technology and information systems, our long-standing fear of human serialization has become more real and immediate. In this respect, the debate over a national identification card offers an opportunity for a long needed debate over the future of privacy in a society that is moving to greater and greater transparency. We need to confront new threats but we also need to maintain those values that allowed us to overcome the scourges of the past.

The most basic foundations for a national identification system are not yet established. Speaking of a national identification system as a general

The Washington Times, July 6, 1999, at 14; Senate to Conduct Hearings on concept is largely meaningless given the wide variety of systems currently in use around the world. Both the constitutional and policy issues raised by such a system in the United States will change dramatically with the adoption of a particular model or the development of a unique system. For example, if a national identification card is needed to allow for speedy identification, it would only require authentication components, such as biometric information. This univocal purpose would not necessarily require databases needed for tracking or significant integration capabilities. If the United States wants to move toward a single integrated system of multiple uses like health care, welfare, or even consumer "smart card" applications, the supporting database network is far more considerable – and potentially controversial.

Our greatest strength as a people has been our creativity and adaptability. By forging a new nation from wilderness, we were less bound by tradition and less fearful of change. Yet, throughout this extraordinary rise as a world power, the United States has remained faithful to its emphasis on the individual over the state. The test of the moment is this: to resist those who threaten our society without changing that society in the process. It remains the great paradox of all free nations. Yet, the Framers never

Abuses by IRS, The Chicago Tribune, September 21, 1997, at 6.

thought this would be an easy road. They merely concluded that it was the only road for a people born to freedom. This was the point that Benjamin Franklin made to a group of citizens who approached him as he left on the final day of the Constitutional Convention. A woman in the crowd asked Franklin, "What have you wrought?" Franklin answered, "a Republic, if you can keep it."[53] Franklin's warning is both chilling and reassuring. Each generation of Americans is given a constitutional legacy that can be nurtured or negated by the exercise of free choice. Ultimately, only the citizens of this country can seriously threaten its foundations. Our charge, as given to us by the Framers, is not only to keep it safe from harm but to pass it along to the next generation in the same condition that it was passed to us.

I would be happy to answer any questions that the Subcommittee may have on this subject.

[53] The Commission on the Bicentennial, The Constitution of the United States 47 (15th ed. 1991).

Mr. HORN. I have had the opportunity last night to read all of them. And we will first get all the presentations in, and the Members will have a question and answer with you and dialog.

Now, my next witness here, we deeply are euphoric, Roy M. Goodman, State senator from New York. You joined us on such short notice. We thank you very much. You flew down here from New York this morning after our invitation yesterday afternoon. So you get things done very fast.

And I look at this background. Any legislator that has 1,200 of his bills become law, that is impressive. So we are lucky around here if we can get five to be presented. And we thank you, because you are also in the same business we are, as chairman of the Senate committee on investigations, taxation and government operations. And looks like you have had a lot of fun. So, thanks for coming.

Mr. GOODMAN. Mr. Chairman, thank you very much indeed for that warm welcome. I am grateful to you and the members of the committee for an opportunity to appear before you today, albeit on relatively short notice.

I would like to make at the outset a comment of warm salute to my former colleague in the State Senate in New York, Major Owens, one of our more esteemed Members who has risen to the heights of the U.S. Congress. Major, I can see just from the height of the ceiling in this room that we have pygmy proportions compared to the stature which all of you possess. And I am very proud to know you.

And also Mrs. Maloney, who happens to be my own Congresswoman, and I very much hope that she will be around in a few moments so I can salute her personally. A much esteemed and good friend, although on the other side of the aisle I must confess.

May I say, Mr. Chairman, that once upon a time on the matter of personal identity, there was a gentleman who entered his men's club, an elderly chap with mutton-chop whiskers, typical of an old Peter Arnaud personality, and he sunk into a deep chair and rang a little bell next to it on the table by which he hoped to summon the club steward so he could order his usual martini. Nothing happened. And he rang the bell again. And finally after ringing it four times, he was outraged, and someone came by and he said, "Great God, man, do you know who I am?" And he spoke to one of the employees in the club. And the chap looked at him and said, "No, sir, I don't, but if you'll go down, I'm sure the gentleman at the front desk will be able to tell you." So this was an indication of an identity crisis that occurred under slightly different circumstances.

May I say, sir, that on a much more serious note, unfortunately, I appear before you at a moment when the Nation is plunged into a war which it did not seek and which was visited upon us in a most astonishing fashion on September 11th. The trauma of that is simply indescribable. I might just tell you that on my first trip down to Ground Zero, I had a chat with the fire commissioner, who was describing some of his experiences on that particular day. Let me say, that he said a chap came up to one of his fireman and said, "I have a helmet here, sir." And he said, "Why are you bothering me with that? We're trying to save lives." He said, "The reason I'm bothering you with that is there is a human head in the helmet."

Alas, the gentleman had been decapitated. And this is one of the horrific, horrendous things that occurred on that day.

And needless to say this is something which has embedded itself in all of our minds most profoundly and with a sense of deep grief and outrage that we appear before you to discuss the problems relating to the identity card matter. And I have to tell you my whole view of it is heavily tainted by the fact that we are at war. I spent 3 years in the Navy during the Korean War and wore about my neck at that time an ID tag with a thumbprint engraved upon it, so that the idea of having a fingerprint identification is certainly nothing new. My officer's identification card had a full set of prints on it. Military service is fully familiar with it.

I thought it would be useful just to take a moment to review with you the contents of my own wallet in regard to cards. I confess I haven't thought to do this until I sat down here this afternoon, but I notice that I have a few of them. And just to give you some idea to the extent to which privacy is invaded, let me give you a quick inventory of my cards. I will make it very brief.

On top is a picture card identifying me as a New York State Senator; driver's license, which also has a picture of me upon it; my Citibank Visa card, which has a picture on it; my MTA, that is to say Metropolitan Transit Authority subway card, which has my picture on it; a Sam's Club card, Sam's Club being a retail establishment where I have credit, which has my picture on it. And we go through a series of others, American Express, New York Society of Securities Analysts, my Medicare card, my New York Public Library card, my Wyoming Public Library card where I go in the summertime, my Barnes and Noble credit card, my New York government employee benefit card, my Automobile Club of America card, my Metropolitan Museum identification card, my Whitney Museum card and my Museum of Modern Art card. Those are just a few of the things I carry with me to be sure that I am at all times able to identify myself as I go about my daily routine.

I think this gives you a little idea of the extent of the lack of privacy which we have. Even with the best of intentions, we are certainly photographed widely, and our data is on file in many different places. I am sure anyone in the room could produce a wallet with somewhat similar credentials and make the point that we are today certainly an identification card society on a very broad level.

And may I say to you, sir, it had been my opportunity as chairman of the investigations committee in 1993 when the World Trade Center was bombed—you may recall that we had a dreadful incident in which there was a gigantic explosion—I went into that hole and found a tremendous crater five stories deep and three stories high and at that time felt it important to examine the matter of how we have achieved security in regard to the terrorist possibilities of future attack. And we prepared a report on that date stating that there were many vulnerabilities and thought it advisable to create a commission, which commission would have as its principal objective the eternal vigilance to try to prevent the recurrence of this type of terrorist attack.

In so doing, I'm sorry to say that peoples' eyes quickly glazed over. And in our world as human beings, we fairly soon forgot that episode, and not until September 11th when we had this far graver problem arise with such unpredicted suddenness do we find ourselves in the position of having to once again reconsider this.

And I did pull together a group of five former police commissioners, group from the FBI and Port Authority, police and a number of others to participate in an examination of potential terrorist targets and possible means of defending against them. That committee happened to have issued a report yesterday, which, if I haven't sent in advance to you, I won't attempt to touch on all aspects because it goes far beyond the subject of today's meeting. But let me say there are at least 50 different ways in which we should be tightening up the security in the State of New York to prevent future occurrences, that cover such things as commercial airline safety, private airline safety, which is a thing that has loopholes the size of the Lincoln tunnel. Anyone can go to a private airport, get on a plane, any size, and load it with any cargo without any inspection whatsoever, proceed to fly over the United Nations building and fly into it, and destroy it in a matter of seconds in much the same fashion that the World Trade Center was destroyed. And the same would apply to the Empire State and others of our magnificent buildings in New York.

This indicates the extent to which in this wartime environment we have not really risen to the concept that we must gird our loins and prepare ourselves with emphatic dedication. I think, as Herbert Spencer said, "It is only by iteration and reiteration that we impress an alien conception upon an unreceptive mind, and it is only by iteration and reiteration that we must remind ourselves we are at war, and war is a very grim business in which we have to suspend values which we normally might wish to feel a repugnancy to us in other contexts."

I see my signal is to stop.

Mr. HORN. Don't worry. Just keep going.

Mr. GOODMAN. I will try to keep it as succinct as I can.

Let me simply say to you that with regard to the matters of other emergency issues, we have looked at hospitals, we looked at the transit system and various matters relating to nuclear/electric/gas supplies for the city of New York. There is a possibility that our power could be shut-off very simply by going to the point of convergence of electric lines.

We want to emphasize the problems of biological and chemical warfare about which much has been, unfortunately, discussed in Washington in the wake of the anthrax scare and on and on.

And let me say that I speak at the moment on behalf of my colleagues who are former police commissioners, as I said, including the new police commissioner designated by our new mayor. His name is Raymond Kelly, and he is an expert in the law, and indeed, I think, is a man of balanced judgment. It was the unanimous judgment of this group that there should be instituted a national identification card system. An open question is whether it should be voluntary or involuntary, and I am not prepared to give you any conclusion, and my own concerns at the moment are very great. As a civil libertarian of longstanding, I am very much concerned about the possibility that such a system could be misused.

But let me just say that, we now have, as Mr. Ellison has pointed out, the means by which to create cards which can carry a tremendous amount of information and certainly establish beyond any reasonable doubt the identity of the individual holding the card. As you may be aware, in Israel, people seeking entrance to an airplane do not have to stand in long lines. They go to a kiosk and insert their card, insert the palm of their hand and stand in front of a camera, which does three things, I am told. One is to check whether the palm print coincides with the print on the electronic chip embedded on the card; to determine whether the facial characteristics are such to be that is the individual involved; and finally, to determine whether the retina of the eye, which is unique in every human being, can positively identify the individual. This tripartite identification concept is one which is now technologically feasible and is in effect in various countries around the world and has been used quite successfully, so that the question is not whether it can be done, nor is it necessarily the cost of doing it, because one could envision a system in which there are payments made as a service as we pay for easy pass cards in our cars going through the toll facilities in New York. So that I am simply here to say to you that the problem becomes one of the extent to which this could impinge on privacy.

And I remind us all that the Supreme Court has stated unequivocally that there is clear protection in the law for privacy, but not for anonymity, and there's nothing about any Supreme Court dicta which I'm aware, and this point is fully emphasized by the distinguished civil libertarian lawyer Alan Dershowitz, who in a paper made it clear that in his judgment the time would come for the use of these cards. And I say to you, sir, it is my belief that in order to accomplish several objectives, the cards may serve a useful purpose, and I would like to quickly outline the objectives, and that will conclude my testimony.

The principal purpose of the card would be to positively identify an individual to be certain that his identity has not been stolen. As you may know, identity theft is a matter that's now quite pervasive in our society. People's identities have been stolen, their bank cards have been lifted, they've been charged with purchases which they never made, telephone calls which they never placed and the like, so that there is a serious problem of finding a stable means of positive identification, which, as I've indicated, now exists. So that the question then becomes one of whether we are in a position to use the cards constructively.

I would say to you that for the privilege of not having to wait 2 to 3 hours on an airline counter line, that might be worth a $25 payment for a lifetime, or 2 or 3-year subscription to a card. Similarly, I think it's quite clear that this would eliminate the need for profiling, an obnoxious thing based upon ethnicity, or the various other characteristics which have been used by police improperly to identify presumed suspects.

By having a positive ID card, a man could walk in wearing all sorts of outlandish clothing, with a beard 3 feet long, and side burns and all the things which might normally be associated with someone who's an undesirable by virtue of easy thinking; and by simply presenting the card, he would exempt himself from the need of any special profiling-type examination.

It strikes me that at this moment, because of the unique facial hirsuteness of the people with whom we are at war, that there is a problem; and as you recall, a Hindu was mistakenly taken for a Muslim and slaughtered early on, right after September 11th, which is the kind of tragedy we certainly wish to avert. An ID card would preclude that type of problem altogether, it's my judgment.

Furthermore, there are various conveniences, if one wished, and wished to volunteer to have certain health aspects of one's existence on the card. If you dropped to the ground with a cardiac arrest and the card were in your possession, it could be put into a reader and quickly determine your condition of health and whether certain drugs that could or could not be administered to you; whether a defibrillator would be an appropriate thing to use in view of your heart rhythm pounding and the like, and this could be a very beneficial health aspect of the card system.

So the point that I'm making is it's not simply an intrusion of privacy that's involved. There are various collateral benefits which should be weighed in a total consideration of whether these cards make sense.

Mr. Chairman, let me just sum up by saying that it's a complex question, and because of my civil libertarian concerns I have thought long and hard about this. I do believe at this time that we have the sufficient sophistication and awareness of the types of problems that exist to formulate a decent judgment in the matter, and I would respectfully suggest to this committee to take a close look at least a volunteer use of such cards. I think at this time, in view of our war emergency, they've become very relevant in attempting to determine who is improperly in the United States at any given moment, tracking people who may be undesirable or have patterns of sabotage or—or other behavior which needs to be properly overseen and tracked, and that without such cards it becomes exponentially much more difficult to accomplish this purpose.

So with those thoughts in mind, I shall now subside with all due respect, and thank you very much for a chance to be heard.

[The prepared statement of Mr. Goodman follows:]

news from

New York State Senate
Committee on Investigations,
Taxation, and Government Operations
Chairman: Senator Roy M. Goodman

NEW YORK CITY OFFICE
31ST FLOOR
633 THIRD AVENUE
(212) 298-5515

ALBANY OFFICE
SUITE 913
LEGISLATIVE OFFICE BLDG.
(518) 455-2211

Contact: Bill O'Reilly, 212-681-0055 FOR IMMEDIATE RELEASE

STATE SENATE ANTI-TERRORISM SUBCOMMITTEE RELEASES PRELIMINARY FINDINGS

Advocates Strong Measures to Protect Public from Further Terrorist Attack

New York, NY—November 15...Senator Roy M. Goodman (R-Manhattan), chairman of the State Senate Committee on Investigations, and a distinguished group of law enforcement officials, today released preliminary findings of the State Senate Anti-Terrorism Subcommittee, which was formed within days of the September 11th attack on the World Trade Center to assess future threats against New York and to recommend steps to improve preparedness.

The committee advocates several major new initiatives. These include adopting procedures for improved commercial and private aviation safety; a national identification card system; expanded use of bomb-sniffing dogs; hospital readiness for medical emergencies; revised transit safety procedures; expanded police cadet program; tightened immigration controls; stronger defenses for nuclear, electric, and gas supplies; improved protections against biological and chemical warfare; and stronger protective measures for public areas, such as malls and stadiums.

The anti-terrorism subcommittee is composed of some of the leading security experts in the nation, including former New York City Police Commissioners Raymond Kelly, Howard Safir, Robert McGuire, Richard Condon, and First Deputy Patrick Kelleher; Port Authority Inspector General Robert Van Etten; former Port Authority Director of Public Safety Henry DeGeneste; Nobel Laureate and bio-science expert Dr. Joshua Lederberg; former State Police Superintendent Tom Constantine; and former New York City Police Chief Michael Schwartz. The Committee is chaired by Senator Roy Goodman and co-chaired by security consultant Robert Strang, formerly of the FBI and DEA.

The special committee, an adjunct to the State Senate Investigations Committee, has met weekly since the attack, questioning experts in key fields and analyzing areas of potential vulnerability to terrorists. The group as a whole has more than 350 years of cumulative professional experience in law enforcement. Its mission is to provide advice to New York State Director of Public Security James Kallstrom and National Homeland Security Director Tom Ridge. In addition, the committee will report to Governor George Pataki, Mayor Rudolph Giuliani, Mayor-elect Michael Bloomberg, Senate Majority Leader Joseph Bruno, and Assembly Speaker Sheldon Silver.

The Committee's preliminary findings and recommendations include:

1. **Adopt procedures for improved commercial airline safety**

   a) Provide federalized supervision of security at all commercial airports.
   b) Provide sky marshals for every commercial flight originating in the United States.
   c) Provide other federal agents to serve as sky marshals until new recruits are trained and placed into service. Possible sources of temporary sky marshals include: law enforcement retirees; U.S. Postal Service armed police; Department of Housing and Urban Development armed agents; and military personnel.
   d) Install security cameras to give cockpit view of what is going on in passenger section.
   e) Upgrade the computer-assisted passenger screening systems (CAPS), which use information obtained in the reservation process to screen out passengers for additional security checks.
   f) X-Ray all checked baggage.
   g) Institute background checks on all airport personnel with access to restricted areas.
   h) Harden all cockpit doors to protect pilots from hijackers.
   i) Require manifest entries for all passengers and crews entering the United States.
   j) Expand use of bomb sniffing dogs to check luggage on airplanes.

2. **Institute immediate surveillance of general (private) aviation**

   a) Survey all private airports and private airplanes, and perform background checks on private pilots.
   b) Determine private ownership of planes.
   c) Check plane leasing and rental arrangements.
   d) Screen cargo and baggage.

3. **Create a system of national identification cards**

   a) Require a universal identification card system initially reading thumb or handprints and ultimately utilizing a high tech electronic chip capable of reading digital fingerprints, digital photographs, and retinal images.
   b) National identification cards will permit us to know who is in the country legally. It will also enable keeping closer watch on those with temporary visas. Such cards would reduce racial and ethnic profiling. The Constitution grants a right to privacy, but does not grant a right to anonymity.

4. **Adopt improved methods to assure public safety**

   a) Expand use of bomb sniffing dogs to check vehicular traffic entering sensitive areas such as tunnels, bridges, and underground garages.
   b) Institute a license plate scanning system to identify all vehicles entering sensitive areas.
   c) Prepare emergency plans to assure rapid entrance and egress of ambulances and other emergency vehicles that enter staging areas to treat the injured in a terrorist attack.

5. **Expanded hospital readiness for emergencies**

   a) Prepare plans for greatly increased patient intake as a result of terrorist attack.
   b) Create special protocols for the handling of pediatric treatment.
   c) Expand blood supply to handle major emergencies. Do not ask public to donate blood when the need does not exist.

6. **Prepare transit safety procedures for subways, buses and commuter railroads**

   a) Promulgate evacuation plans for subways, buses, and commuter railroads.
   b) Ensure adequate ventilation in stations and tunnels in the event of fires or gas attacks.
   c) Require background checks on all employees working in the transportation system.

7. **Increase manpower availability and mobilization**

   a) Utilize and expand the police cadet and ROTC programs for anti-terrorist patrol and related law enforcement activities.

8. **Tighten immigration procedures**

   a) Impose tighter control over issuance of visas.
   b) Identify and monitor activities of immigrants considered high-risk visitors.
   c) Tighten procedures at major entry points such as the Canadian and Mexican borders.

9. **Create stronger defense for nuclear, electric, and gas supplies**

   a) Identify and secure points where electricity supply lines converge.
   b) Survey upstate power lines, which run for hundreds of miles through open land.
   c) Utilize fly over patrols and improved surveillance cameras to identify vulnerabilities.
   d) Increase armed guard force to provide 24-hour protection for crucial power towers.
   e) Circulate instructions for radiation protection and other special procedures for nuclear defense.

10. **Emphasize prevention rather than response to attacks**

   a) Identify high risk targets by conducting regular and ongoing audits, as was done by state and city police in preparation for Y2K.
   b) Appoint permanent committee of law enforcement experts to provide terrorist threat assessment and preparedness.
   c) Assure that agencies have drills to prepare for orderly implementation of emergency procedures.
   d) Ensure that all relevant intelligence is shared among national, state, and local law enforcement agencies, subject to appropriate safeguarding of sources.

11. **Improve protections against biological and chemical warfare**

   a) Accelerate anthrax research to determine vectors of transmission and to develop more rapid and accurate testing.
   b) Conduct surveys of vulnerability to smallpox and other diseases to assure rapid availability of counter measures if necessary.
   c) Stockpile necessary supply levels of vaccines and other medication.

12. **Adopt protective measures for shopping malls, stadiums, arenas, auditoriums, and other places of public gathering**

   a) Prepare crisis plans and conduct appropriate evacuation drills.
   b) Provide emergency shelters where necessary.

13. Pass corporate hold-harmless legislation

a) Provide exemption from lawsuits for corporations that follow guidelines for coping with terrorist threats. This will eliminate corporate need overreaction to threats, which would have the effect of swamping hospitals.

14. Strengthen the capability of law enforcement at the local level

a) Review existing state laws to ensure that they replicate federal counter terrorist measures.
b) Increase assets of state and local law enforcement to assist in intelligence gathering.
c) Develop state legislation to monitor the financial transactions of suspected terrorists.

###

Mr. HORN. I think you mentioned earlier that you had some recommendations out of your committee and once you're done with it, if you could, we will have a spot in this to get the whole document.

Mr. GOODMAN. I will be glad to do that, sir.

Mr. HORN. Thank you very much.

Mrs. MALONEY. Can I have a personal privilege? I would——

Mr. HORN. He says he likes you now.

Mrs. MALONEY. Well, I would like to welcome——

Mr. GOODMAN. While you were out of the room, Congresswoman, I took the liberty of saluting you most warmly.

Mrs. MALONEY [continuing]. Over the years, and we welcome your testimony. You've always tackled the hard problems and come up with good answers, and we appreciate your distinguished input into this committee. Thank you for coming and it's good to see you.

Mr. GOODMAN. Thank you very much. It's very good to see you, too.

Mr. HORN. We now go to Katie Corrigan, who is the legislative counsel on the privacy issues for the Washington National Office of the American Civil Liberties Union, and she has quite a background in terms of health, education, labor, pensions matters, and we're glad to have you here.

Ms. CORRIGAN. Thank you. Thank you, Mr. Chairman, and thank you members of the subcommittee. I appreciate the opportunity to testify before you on National ID proposals on behalf of the American Civil Liberties Union.

The ACLU is a nationwide nonpartisan organization with nearly 300,000 members dedicated to protecting the individual liberties and freedoms guaranteed in the Constitution and the laws of the United States.

Like all Americans, the ACLU supports efforts to ensure our security from terrorist threat but we remain convinced that we need not sacrifice our liberties to protect our safety. We believe a national ID system in any form should be rejected.

First, ACLU believes that the threshold question is whether or not a security measure would be effective at protecting us from terrorist threat. Since the terrible events of September 11th, there have been numerous proposals to create a national ID system. The rationale is that we need to create a clear line between us—the innocent people—and them—the dangerous terrorists. Every one of us would like an ID card that would put us squarely on the right side of the line and exempt us from suspicion and heightened security when we board a plane or go to work.

Unfortunately, none of the proposed ID systems would effectively sort out the good from the bad. An identity card is only as good as the information that establishes an individual's identity in the first place. It makes no sense to build a national ID system on a faulty foundation, particularly when possession of the ID card would give us a free pass to board a plane or avoid security checks at Federal buildings or other public places.

No form of documentation is completely foolproof. The same people who are forging ID's today will forge them tomorrow. There are always ways to beat the system. Presumably an individual would obtain an identity card, using a document such as birth certificates or a driver's license. Anyone, including terrorists, could alter or obtain such documents.

The Inspector General of Social Security testified last week that six of the hijackers obtained Social Security numbers through fraudulent means, and, as U.S. citizens, domestic terrorists like Timothy McVeigh would certainly qualify for an ID.

Second, not only would a national ID create a false sense of security but it would be very, very expensive and divert resources from perhaps more effective counterterrorism measures. In 1998, the GAO reported that the Social Security Administration estimates no matter what material a card is made from or what type of technology, including biometrics, is used for security, issuing an enhanced card to all number holders using current procedures would cost a minimum of about $4 billion or more. And even with the offer from Oracle and Larry Ellison for free software, the processing costs alone of issuing new ID's to Americans are estimated to be 90 percent of that billion dollar expense.

Third, in addition to huge costs, a National ID would require a massive identification bureaucracy to support it. Thousands of government employees would be required to develop, implement, maintain, the supporting computer infrastructure and technology standards for the ID cards. The SSA's $4 billion estimate didn't even consider the cost of updating the picture or other identifiers on the card over a person's lifetime, or periodically replacing the magnetic strip on the back, or the simple cost of having to replace lost or stolen ID's.

When setting up any new bureaucracies, simple questions need answers. What would happen if an ID card is stolen? What proof of identity would be used to decide who gets a card? What would happen if you lose your ID? Anyone who has had to correct an inaccurate credit history will understand how hard it could be to correct an error that has found its way into a government data base. Error rates and government data bases already tend to be especially high, and we heard that from members of our first panel. Then what happens if you are misidentified or one of the thousands of victims of identity theft? Even with a biometric identifier on each and every ID, experts say there's no guarantee that individuals will be identified or misidentified in error. A technology expert at the University of Pennsylvania recently said biometrics are fallible.

Fourth, an ID system violates basic American values including, our privacy, our quality, and our right simply to be left alone. Day-to-day individuals could be asked for ID when they are walking down the street, applying for a job or health insurance or entering a building. This type of intrusiveness would be joined with the full power of modern computer and data base technologies. How long before office buildings, doctors' offices, gas stations, highway tolls, subways, and buses incorporate the ID card into their security or payment systems? The result could be a Nation where citizens' movements inside our own country are monitored through what would equivalently be internal passports. The data base supporting such an ID system would be massive and contain all sorts of highly personal information. Thousands and thousands of government employees and even private industries could have access to it.

The scope of information accessible through a centralized data base as opposed to the many different data bases that are attached to the cards that Senator Goodman pointed to would magnify the risks of privacy violations. One mistake by a government employee could result in disclosure of personal information that could follow you around the rest of your life.

This past month, a State university accidentally posted the psychological records of 62 children on the Internet, names, addresses, along with intimate details such as "a boy prone to anger outbursts, gender identity issues and bed wetting." Disclosures could come back to haunt children later in life when they're trying to find a job or get a security clearance. With an ID system, one accidental keyboard stroke could put a person's most sensitive information into public distribution.

And finally, Mr. Chairman, some people have argued that ID cards would end racial profiling and other discriminatory practices. Unfortunately, we believe that cards would provide new opportunities for discrimination and harassment of people who are perceived as looking or sounding foreign.

The 1986 requirement that employers verify the identity of potential employees and their eligibility to work in the United States has resulted in widespread discrimination against foreign-looking American workers, especially Asians and Hispanics. A national ID card would have the same effect on a broader scale. Latinos, Asians, African Americans, and other minorities would become subject to more and more status and identity checks. This would have a stigmatizing and humiliating effect and undermine our right to equal treatment. The national ID system in any form could be expensive, require a cumbersome bureaucracy, and violate some of our fundamental American values, and it simply wouldn't work to stop terrorism.

The ACLU urges the Congress to reject proposals for a national ID system. And I would be happy to answer any questions at the appropriate time. Thank you.

Mr. HORN. Delighted to have your presentation.

[The prepared statement of Ms. Corrigan follows:]

AMERICAN CIVIL LIBERTIES UNION

WASHINGTON NATIONAL OFFICE
Laura W. Murphy
Director

122 Maryland Avenue, NE Washington, D.C. 20002
(202) 544-1681 Fax (202) 546-0738

STATEMENT

OF

KATIE CORRIGAN

LEGISLATIVE COUNSEL

AMERICAN CIVIL LIBERTIES UNION

WASHINGTON NATIONAL OFFICE

ON

DOES AMERICA NEED A NATIONAL IDENTIFIER?

BEFORE

GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND

INTERGOVERNMENTAL RELATIONS SUBCOMMITTEE OF THE

HOUSE OF REPRESENTATIVES COMMITTEE ON GOVERNMENT REFORM

NOVEMBER 16, 2001

AMERICAN CIVIL LIBERTIES UNION

WASHINGTON NATIONAL OFFICE
Laura W. Murphy
Director

122 Maryland Avenue, NE Washington, D.C. 20002 (202) 544-1681 Fax (202) 546-0738

My name is Katie Corrigan and I am the legislative counsel on privacy at the American Civil Liberties Union (ACLU). The ACLU is nationwide, non-partisan organization with nearly 300,000 members dedicated to protecting the individual liberties and freedoms guaranteed in the Constitution and laws of the United States. I appreciate the opportunity to testify today on recent proposals to establish a national identification system or national ID card. Like all Americans, the ACLU supports efforts to ensure our security from terrorist threat; but we remain convinced that we need not sacrifice our civil liberties to protect safety. We believe our country can be both safe and free.

We ask Congress to use a three-prong analysis to promote safety and to reduce the likelihood that new security measures would violate civil liberties.

First, any new security proposals must be genuinely effective, rather than creating a false sense of security. Second, security measures should be implemented in a non-discriminatory manner. Individuals should not be subjected to intrusive searches or questioning based on race, ethnic origin or religion. Finally, if a security measure is determined to be genuinely effective, the government should work to ensure that its implementation minimizes its cost to our fundamental freedoms, including the rights to due process, privacy and equality.

A national identification card does not pass these basic tests. A national ID card would substantially infringe on the rights of privacy and equality of many Americans, yet would not prevent terrorist attacks. The ACLU strongly opposes the creation of a national ID card, whether the card is embodied in plastic, or whether the "card" is intangible – a sort of "virtual reality" card consisting instead of a government-mandated computerized database containing information about most people in the United States linked by a government-issued identifier.

Over the past few decades, proposals for a national identification system have appeared as a "quick fix" to a national problem of tracking one segment of the population or another, including immigrants and deadbeat dads. Since September 11, national ID proposals have been discussed in the media and in the Congress as possible counterterrorism measures. (See Appendix.)

NATIONAL ID CARD OR SYSTEM WOULD BE AN INEFFECTIVE COUNTERTERRORISM MEASURE AND WOULD SERIOUSLY UNDERMINE BASIC LIBERTIES

A national ID card or system would not be an effective counterterrorism measure. Instead, such a system could divert resources away from other counterterrorism activities and create a government bureaucracy that would undermine basic rights to privacy and equality.

First, national ID cards would create a false sense of security and divert valuable resources from other more effective counterterrorism efforts.

The rationale for creating a national ID system post-September 11 is to create a clear line between "us" (innocent people) and "them" (dangerous terrorists). Everyone would like an ID card that would put them squarely on the right side of the line and exempt them from suspicion and heightened security scrutiny when they board a plane or go to work.

Unfortunately, none of the proposed identification systems would effectively sort out the "good" from the "bad." First, an identification card simply confirms that you are who you say you are. It does not establish motive or intent to attack a plane. All 19 of the September 11 hijackers had social security numbers (SSNs), although not all of them were legitimate. One of the hijackers was listed in the San Diego phone book – both name and address. And still others rented automobiles with their debit cards and lived in suburban Florida neighborhoods. But only a few of the hijackers were on FBI watch lists. An ID card would simply have reaffirmed the hijackers' real or assumed identities. It would have done nothing to establish their criminal motives for renting cars and going to flight school.

Second, an identity card is only as good as the information that establishes an individual's identity in the first place. It does not make sense to build a national identification system on a faulty foundation, particularly when possession of an ID card would give you a free pass to avoid heightened security measures.

No form of documentation is completely foolproof. There are always ways to beat the system. Presumably, an individual would obtain an identity card using documents such as a birth certificate or driver's license. Anyone, including terrorists, could falsify or forge such documents. The Inspector General of the Social Security Administration testified last week that six of the hijackers obtained SSNs through fraudulent means.[1] And, at least one person who is a suspected associate in the September 11 attack has been indicted for using false information to obtain a SSN. In addition, a national ID card would do nothing to sort out domestic terrorists. As a US citizen, Timothy McVeigh would have certainly qualified for a national ID.

A national ID system would inevitably foster the blackmarket in fake identification. For instance, in 1990, several DMV employees in Virginia were indicted for selling possibly thousands of drivers' licenses to illegal immigrants in violation of the law.[2] The creation of these cards and supporting infrastructures create new risks of insiders issuing phony IDs and outsiders gaining access. There is always the potential for misuse by individuals in any large organization.

At best, a national ID would serve as a placebo to make us all feel better when we show the card at the airport, a turnpike tollbooth, or at our workplaces. At worst, the ID card would create a false sense of security and divert resources from other more productive counterterrorism activities. In 1998, General Accounting Office (GAO) reported that mass issuance of counterfeit-resistant Social Security cards would be very

[1] *Hearing on Social Security Administration's Response to the September 11, 2001, Terrorist Attacks before the Subcommittee on Social Security of the House Committee on Ways and Means*, 107th Cong. (Nov. 1, 2001) (statements of Hon. James G. Huse, Jr., Inspector General, Office of Inspector General, Social Security Administration).

[2] Frank Wolfe, *Drivers license scam busted*, WASH. TIMES, Dec. 7, 1990.

expensive.[3] The Social Security Administration estimated that no matter what material the card was made from or what type of technology was used for security purposes, such as biometric identifiers, "issuing an enhanced card to all number holders using current procedures would cost a minimum of about $4 billion or more." And, even with the offer from Larry Ellison (Chairman and CEO of Oracle) of free database software, the processing costs alone of issuing new ID cards are estimated to be 90% of the $4 billion expense.

Second, national ID cards would provide a new tool for racial and ethnic profiling and lead to more illegal discrimination, not less.

The cards would provide new opportunities for discrimination and harassment of people who are perceived as looking or sounding "foreign." Some people have argued that ID cards would end racial profiling and other discriminatory practices. We need only look to history to see how "identification" requirements can impact the daily lives of Americans. The Immigration Reform and Control Act of 1986 required employers to verify the identity of potential employees and their eligibility to work in the U.S. The Act also imposed sanctions for failing to comply with the verification requirements. As a result, there has been widespread discrimination based on citizenship status and against foreign-looking American workers, especially Asians and Hispanics. A 1990 General Accounting Office (GAO) study found almost 20 percent of employers engaged in such practices.[4]

A national ID card would have the same effect on a broader scale. Latinos, Asians, African-Americans and other minorities would become subject to more and more status and identity checks -- not just from their employers, but also from police, banks, merchants and others. The failure to carry a national I.D. card would likely come to be viewed as a reason for search, detention or arrest of minorities. This would mean certain individuals, including immigrants, would be increasingly vulnerable to a system that subjected them the stigma and humiliation of constantly having to prove their citizenship or legal immigrant status.

Third, massive databases of information are a direct threat to the privacy of average Americans and the basic freedom to move freely around our neighborhoods and towns.

A national ID system would violate the freedom Americans take the most for granted and the one that most defines our liberty: the right to be left alone. Unlike workers in Nazi Germany, Soviet Russia, apartheid South Africa, and Castro's Cuba, no American need fear the demand, "Papers, please." As a free society, we cherish the right to be individuals, to be left alone, and to start over, free from the prying eyes of the government.

[3] 1998 GEN. ACCT. OFF. REP. NO. GAO/HEHS-98-170, SOCIAL SECURITY: MASS ISSUANCE OF COUNTERFEIT-RESISTANT CARDS EXPENSIVE, BUT ALTERNATIVES EXIST.

[4] 1990 GEN. ACCT. OFF. REP. NO. GAO/GGD-90-62, IMMIGRATION REFORM: EMPLOYER SANCTIONS AND THE QUESTION OF DISCRIMINATION.

As former California Representative Tom Campbell recently argued, "If you have an ID card, it is solely for the purpose of allowing the government to compel you to produce it. This would essentially give the government the power to demand that we show our papers. It is a very dangerous thing."[5]

Internal Passports Required: A national ID card would set up the infrastructure for a surveillance society. Day to day, individuals could be asked for ID when they are walking down the street, applying for a job or health insurance, or entering a building. This type of daily intrusiveness would be joined with the full power of modern computer and database technology. If a police officer or security guard scans your ID card with a pocket bar-code reader, for example, will a permanent record be created of that check, including the time and location? How long before office buildings, doctors' offices, gas stations, highway tolls, subways and buses incorporate the ID card into their security or payment systems for greater efficiency? The result could be a nation where citizens' movements inside their own country are monitored and recorded through these "internal passports."

Misuse of Highly Personal Information: Once all of this information is in the government databases, there is no guarantee its use would be limited to protecting security. There are clear examples of how government-collected information has been used for purposes other than that which it was originally intended. For instance, the confidentiality of Census Bureau information was violated during World War II to help the War Department locate Japanese-Americans so they could forcibly be removed to internment camps. During the Vietnam War, the FBI secretly operated the "Stop Index" by using its computerized National Crime Information Center (NCIC) to track and monitor the activities of people opposed to the United State's involvement in the war.

Everyday privacy violations victimize average Americans and undermine public confidence in the government. Thousands and thousands of government officials and perhaps even private industry would have access to a massive database of personal information required to support a national ID system. Even now internal breaches of database information happen all the time at the federal and state levels. In 1997, the General Accounting Office found serious weaknesses in the IRS' computer security and privacy protections and a year later many of the problems remained.[6] Just last week, a former top Chicago detective admitted to running a jewel-theft ring across several states for more than a decade. Prosecutors said the detective had used law enforcement and other databases to get information about the travel schedules of traveling jewelry salesmen.[7] And, an investigation by the Detroit Free Press shows other types of abuses that can happen. Looking at how a database available to Michigan law enforcement was used, the newspaper found that officers had used it to help their friends or themselves stalk women, threaten motorists, track estranged spouses – even to intimidate political opponents.

Even an innocent mistake by a single government employee can have a huge impact on an individual's life. In the past month, the University of Montana accidentally posted the psychological records

[5] Paul Rogers & Elise Ackerman, *National ID Prompts Feasibility Doubts in Technology Industry*, SAN JOSE MERC. NEWS, Sept. 25, 2001.

[6] 1998 GEN. ACCT. OFF. REP. NO GAO/IMD-99-38, IRS SYSTEMS SECURITY: ALTHOUGH SIGNIFICANT IMPROVEMENTS MADE, TAX PROCESSING OPERATIONS AND DATA STILL AT SERIOUS RISK.

[7] John W. Fountain, *Former Top Chicago Detective Admits to Leading Theft Ring*, N.Y. TIMES, Oct. 26, 2001.

of 62 children on the Internet. Names, addresses, and psychological tests were posted along with intimate details such as the boy prone to "anger outbursts, gender identity issues" and bedwetting. The immediate impact of such disclosures includes embarrassment and humiliation or further psychological trauma. The long term impact could be depression, poor performance in school and, depending on which databases the psychological information ended up, it could come back to haunt children later in life when they are trying to find a job or get a security clearance.

Any one of these privacy violations would be magnified in the context of a national ID system. A national ID system would allow government officials to access information contained in numerous and unrelated databases through one centralized system. Fraud or mistake would no longer be limited to one state law enforcement database or one university's research files. Government employees could tap into a database that included all kinds of information about an individual – from tax returns to health care data to student loan information. One employee or one wrong keyboard stroke could send a person's entire file into public distribution.

Finally, national ID proposals ask Americans to trust that a massive identification bureaucracy would facilitate our way of life rather than undermine the freedoms we take for granted.

The scale of the bureaucracy required to implement a national ID system cannot be underestimated. Thousands of government employees would be required to develop, implement, and maintain the supporting computer infrastructure and technology standards and process the cards for every American. The SSA estimated the cost of issuing counterfeit-resistant social security cards at $4 billion. The Administration did not even consider, however, the cost of updating the picture or other identifier on the card over a person's lifetime, periodically replacing the magnetic or electronic storage technology to ensure reliability, or the simple costs of having to replace lost cards.[8] In addition, this report did not consider the information database that would also have to be developed, implemented, and maintained.

What would happen if an ID card is stolen? What proof of identity would be used to decide who gets a card? What would happen if you lose your ID? An overnight business trip might have to be cancelled because you don't have the time to go through heightened security at the airport. You might not be able to drive across a bridge to work without ID that says you are who you say you are. Even worse, you might not be employable without proof of ID. And, what if you run out of your house to buy a quart of milk and forget your ID? If a police officer stops you, you would automatically be considered suspect.

Anyone who has had to correct an inaccurate credit history will understand how hard it could be to correct an error that has found its way into your national ID file. Error rates in government databases tend to be high. Internal Revenue Service data and programs have been found to have error rates in the range of 10 to 20%.[9] And, according to the GAO, there has been a significant increase in identity theft over the years.[10] It is

[8] *See* note 3.

[9] John J. Miller and Stephen Moore, *A National ID System: Big Brother's Solution to Illegal Immigration*, Cato Policy Analysis No. 237, Sept. 7, 1995.

[10] 1998 GEN. ACCT. OFF. REP. NO. GAO/GGD-98-100BR, IDENTITY FRAUD.

estimated that 40,000 victims of identity theft must struggle each year to clear their names and fix their credit histories.

Even with biometric identifiers on each and every ID, experts say there is no guarantee that individuals won't be identified – or misidentified -- in error. Professor David J. Farber, a technology expert at the University of Pennsylvania recently said, "Biometrics are fallible."[11] Fingerprints and retinal scans are reasonably reliable when used with an expensive reader. Other forms of biometrics such as hand readers and facial recognition, however, have high error rates. (See ACLU's Feature on Facial Recognition Technology at http://www.aclu.org/features/f110101a.html.)

Under a national ID system, employee mistake, database error rates, and common fraud would not simply affect individuals in one area of life. Instead, problems with the ID system or card could take away an individual's ability to move freely from place to place or even make someone unemployable until the file got straightened out.

The proponents of a national identification system argue that our circumstances have changed since September 11, and now Americans must accept "a little less anonymity for a lot more security." Unfortunately, this trade-off is rooted in the false assumption that a national ID card would make us more secure and fails to account for the full range of civil liberties at stake in this debate.

HISTORY OF THE SSN POINTS TO PROBLEMS WITH NATIONAL ID SYSTEM

A "Golden Rule" of informational privacy is that information collected by the government for one purpose should not be used for another purpose without the consent of the person to whom such information pertains. The history of the Social Security Number (SSN) shows just how difficult it is for the government and private industry to abide by this simple rule. It also documents Congress' longtime resistance to national ID systems.

In 1935, the Social Security Number (SSN) was created solely for the purpose of tracking contributions to the social security fund. But as soon as 1943, President Roosevelt issued an Executive Order encouraging other federal agencies to use the SSN when establishing a "one system of permanent account numbers pertaining to an individual's person." In 1961, the Civil Service Commission began using the number to identify all federal employees. The next year the IRS required the number on all individual tax returns. And, by the mid-1960s, the use of the SSN exploded in both the public and private sector as the introduction of the computer coincided with the expansion of government assistance programs.

Based on reports from the Administration and congressional hearings, Congress realized the SSN posed grave privacy concerns for the American public. In response, Congress enacted the Privacy Act in 1974 based on a finding that the right to privacy was "directly affected by the collection, maintenance, use and dissemination of personal information by federal agencies," and that the increasing use of computers and

[11] Lorraine Woellert, *Commentary: National Ids Won't Work*, BUS. WK., Nov. 5, 2001.

sophisticated information technology "greatly magnifies the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information."

Of course, Congress has considered numerous proposals to institutionalize the SSN as a national ID and consistently rejected them. Most memorably, President Clinton proposed a health security card as part of his nationalized health care plan. Both proposals met strong opposition and became a symbol of big government.

Most dramatically, in 1996 the House of Representatives rejected national ID cards during the consideration of the Illegal Immigration Reform and Immigrant Responsibility Act (HR 2202, 104th Congress). Rep. McCollum (R-FL) offered an amendment "to make a Social Security card as counterfeit-proof as the $100 bill ... and as free and protected from fraudulent use as a passport."[12] The Commissioner of Social Security opposed the amendment because the Administration was opposed "to the establishment, both de jure and de facto, of the Social Security card as a "National Identification document."[13] The Administrator also pointed out that SSA already included most of the anti-fraud features of the $100 bill.

Most recently, in 1999, a left-right coalition worked with Members on both sides of the aisle to repeal a provision in the 1996 Illegal Immigration and Immigrant Responsibility Reform Act that effectively coerced every state to place SSNs on every driver's license.

The lesson of the SSN is that once Congress establishes an infrastructure for tracking citizens, even if privacy protections are included, efficiency-driven "mission creep" turns a limited tool into a broad-based assault on privacy.

CONCLUSION

Congress should not set us on a track that would undermine our privacy, threaten equality, and challenge our very understanding of freedom. The ACLU strongly believes that our country must be safe, but security measures must be effective and need not come at the cost of our fundamental liberties. Congress should reject national identification systems in any form.

Thank you for inviting me to testify today. I am happy to answer any questions.

[12] 142 CONG. REC. H2452, (daily ed. March 19, 1996).

[13] Letter from Shirley S. Chater, Commissioner, Social Security Administration, to the Honorable Jim Bunning, (March 19,1996)(published in 142 CONG. REC. H2452, (daily ed. March 19, 1996)).

APPENDIX: NATIONAL ID PROPOSALS IN THE MEDIA AND BEFORE CONGRESS

The various national ID proposals differ in kind, but not in effect. Almost all of them would centralize individuals' highly personal information, such as tax information, health and social security information, and law enforcement data, into an integrated database. The government would issue individuals an ID card with a unique identifier that could access all of the various databases to confirm identity, run background checks, or administer government benefits.

National ID Card Proposals

"The Ellison National ID" Proposal: Larry Ellison, Chairman and CEO of Oracle, has offered to provide the US government with the necessary software to build a national identification system. Ellison recently wrote in the Wall Street Journal, "[t]he single thing we could do to make life tougher for terrorists would be to ensure that all the information in myriad government databases [at the federal, state and local level] was integrated into a single national file."[14] This database could be connected to a digital ID card that would replace Social Security cards and drivers' licenses. It could also be used to speed up the security check-in at airports and used by private industry for company ID cards.

"The Dershowitz National ID" Proposal: Professor Alan Dershowitz has provided fewer specifics on his national ID proposal, but would appear to agree with Ellison's general concept. A national ID would not be mandatory, but it would "allow [individuals] to pass through airports or building securities more expeditiously, and anyone who opted out could be examined much more closely."[15]

National ID Card Proposals by Another Name

No Member of Congress has introduced legislation that would implement a national ID system or ID card. Instead, there are several proposals that would establish a national ID card or system through the "backdoor" of other proposed legislation.

"The Trusted Passenger" National ID: Section 109 of the House air security bill, H.R. 3150 the "Secure Transportation for America Act," allows the Department of Transportation to implement a "trusted

[14] Larry Ellison, *Smart Cards, Digital Ids Can Help Prevent Terrorism*, WALL ST. J., Oct. 18, 2001.

[15] Alan Dershowitz, *Why Fear National IDs?*, N.Y. TIMES, Oct. 13, 2001. Both Ellison and Dershowitz emphasize that their ID card systems would be "voluntary." This distinction, however, is without practical meaning. "Voluntary" ID cards would quickly become a de facto requirement for conducting all kinds of daily activities. As adoption of the card spreads, those who decide not to "volunteer" for such a card will increasingly find themselves subject to intrusive, humiliating, and time-consuming searches or even denied access to certain services and buildings - in short, treated like second-class citizens. In time, Americans will be for all practical purposes forced to acquire a card and to submit to whatever procedures are used to issue them.

passenger program." The text of the legislation fails to detail the elements of the program, but its purpose would be to expedite airport screening by establishing the identity of "trusted" passengers through the issuance of an ID card. The ACLU explained in a letter to the air security conferees last week that the trusted passenger program could easily be extended to all types of travel, making it more difficult to move freely around the country, a state, or even a locality without such a trusted passenger ID. As a result, the trusted passenger program could become a de facto national ID system, requiring Americans to carry an internal passport with them wherever they go. This sytem won't stop terrorists. Too often, "trusted passengers" simply can't be trusted.

The Air Transport Association National ID: Last week, the Air Transport Association, the industry group for airline carriers, announced its support for a similar "National Traveler's ID."[16] CEO Carol Hallett called on the federal government to develop a "constantly refreshed" database that would include law enforcement data, immigrations and customs information, treasury and financial data and "any other databases the government requires." Not unlike Ellison's proposal, the "Federal Information System" database would go along with an ID card containing biometric identifiers and other anti-counterfeit technologies.

Once such a massive database is established, the traveler's ID wouldn't be limited to aviation security for long. Hallett herself said, "All of the activities I have described ultimately should benefit homeland security and national security, not just aviation security."

Feinstein/Kyl National ID Starter Kit: Earlier this month, Senators Feinstein and Kyl introduced the "Visa Entry Reform Act of 2001" (S. 1627). The purpose of the bill is to strengthen counterterrorism efforts at our borders and in the visa process. The bill includes a centralized "lookout" database that would contain information about foreign nationals crossing the border into the United States. In addition, the Feinstein/Kyl bill establishes a "SmartVisa" card to make newly issued visas tamper-proof and counterfeit-resistant using biometric identifiers.

Section 7 of the Feinstein/Kyl bill, however, goes far beyond immigration policy and mandates uniform procedures for identification cards and other government documents used by average Americans. The bill clearly contemplates the "next step" toward a national ID.[17]

Section 7 requires the Attorney General to establish uniform procedures to "prevent fraudulent use and alteration by tampering" for "newly issued identification documents, licenses, and permits" issued by the Department of Justice, Department of Transportation, Department of Health and Human Services, and the Social Security Administration.

This provision would require the federal agencies to follow a uniform identification system for individuals obtaining government services including Medicare payments and social security benefits, or other

[16] Press Release, Air Transport Association (Nov. 11, 2001)(release can be found at www.air-transport.org/public/news/display2.asp?nid=4710).

[17] In a *Los Angeles Times* article, Senator Feinstein described her proposal for an immigrant ID card saying, "It's just for people coming into the country ... I think this is where we should start." Joseph Menn, *National ID Card System Failing to Attract Supporters*, L.A. TIMES, Oct. 24, 2001.

permits and licenses. Section 7 also requires state and local governments to meet the federal requirements for any state or local identification documents subject to "Federal requirements or standards." That means the federally-mandated uniform identifier would apply to documents such as state-issued commercial trucking licenses or professional medical licenses subject to federal minimum standards.

This provision lays the groundwork for the implementation of broad-based uniform identification requirements (i.e. a national ID system) at the federal, state and local level. Congress already rejected a similar mandate to the states when it repealed Section 656(b) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996.

Driver's License National ID: The American Association of Motor Vehicle Administrators (AAMVA) has advocated a national standard for state drivers' licenses. The proposed standards include both uniform identification requirements for the holder of the driver's license, including name, address, and personal characteristics, and uniform technology standards for additional data storage on the card, such as bar codes and optical memory.

The AAMVA itself has stated its proposal for standardized drivers' licenses would effectively create a national ID card.[18]

[18] Alan Gathright, *Biometric technology raises hopes, fears, and skepticism*, S.F. CHRON., Oct. 30, 2001.

Mr. HORN. And we now move to Rudi Veestraeten, the Counselor and Consul at the Embassy of Belgium, and he's been in their Foreign Affairs Ministry in their home city, and he's had quite a career for his own country, and we're thanking you for telling us how that works.

Mr. VEESTRAETEN. Thank you, Mr. Chairman. Thank you, members of the subcommittee. It's an honor to be invited here today. I'll try to give some comments. A document which was distributed contains the basics about the system in Belgium.

First of all, Belgium is—for those who doubt, is a democracy. It's a democratic country. We have a longstanding record of democracy and, specifically, we have a very longstanding record of registering people and issuing ID cards. We actually started issuing ID cards in 1919. We started registering people locally in towns and in cities in 1856. That is an existing system in Belgium.

I think when we talk about ID cards, when we talk about registration, there are—and we talk about the events of September 11th and other threats in the society today, there are in fact three elements which are often mixed: First, there is the ID card as such. The ID card is just a document which allows somebody to identify who he is; 100 years ago, 50 years ago, people might still just know you or know who you are. Even today people in my village in Belgium, they know who I am. My neighbors here in McLean know who I am. But when I drive around in a car, people do not know anymore. The card is just a means to prove who you are, that you are who you say you are. That is the card.

And then the second element in this discussion, the data base issue. We also have a quite sophisticated system in Belgium with a centralized data base which contains a limited amount of information you can find out in the documentation. The data base is a very powerful tool to quickly find more. If somebody shows up and has an identity card, you can then as a police officer, as a public servant, depending on what your duties are, you can find out about that person, what his background is. This data is not contained in the cards, not written on the cards, but there is a whole data base behind the card, a system where more information is available if needed, to those who need it.

And then there is the whole issue of security, and I'm not going to talk about that.

Of course, the fact of having a card, having a passport, having a travel document, having a driver's license, does not allow any police officers to determine whether a person is a terrorist or a genuine person. That's not the purpose of the cards, let's not mistake this. The purpose of the card is only to identify that this person does have this first name and that last name, and is probably registered at a particular address. That's a very important distinction to make, I think.

If we discuss abuse of the cards, I mean the threats of having a card in a country like Belgium, the threat of having this system where everybody needs to carry the cards, well, in fact, you can say the same—this dates back from the German occupation. We were occupied by the Germans twice, in 1418 and in 1940–1945. We have been fighting the German system, the Nazism, the fascists in 1940–1945, and we are proud to have done that. I think we have a longstanding record of fighting authoritarian mechanisms, authoritarian regimes, and we are very proud of that.

Now, the Germans, when they have occupied Belgium, they used police, they used military police, they used an army to occupy our country and to take away all our civil liberties. Now, this does not mean that we have decided after we are freed from the German occupation to abolish police, to do away with an army, to do away with military police. That's not to the point. What we should try to do is to keep steady democratic control over what police do in our country, keep steady democratic control about what the army is doing, what the army can do, what powers the army can be given. And that is the sense of the—it's not about having a police which can, of course, abuse its force; it's about control of the police.

The same goes, in our view in Belgium, for the cards. It's not about the cards. It's about how you use the cards, what you allow people to do with the cards, what you control and so on. That is the essence of the debate in our country where it was taken.

Now, if we want to see what the card means in our system today, what do we use it for, I think the best way to—and for the 2 minutes I have left, to explain—that is, to see, to imagine from my viewpoint, for me to imagine my country without the identity cards, what would be the difference if you would take away the identity cards in Belgium. I think, first of all, we would do what is the case in many other countries. We would probably see other documents being used instead of an identity card. This might be drivers' licenses, this might be Social Security cards. We have those cards in Belgium as well. The problem there—and that is why we have introduced the card in the first place.

The problem is that those other cards contain data which are not meant to be communicated to other people. I mean, on a driver's license, there can be data which are not meant to be communicated to a bank employee. It can be medical data, like vision. It can be—it can appear to be not very important, but the vision is mentioned on the driver's license.

The same goes for the handicapped, in some cases. I mean, drivers' licenses are meant for other purposes other than identification, and therefore contain other information which are not meant for public distribution and not meant for the bank employee.

The same goes for security. The other cards, Social Security card here and in Belgium, those cards are not meant for identification purposes and so do not contain the proper security features which would be required for an identity card, which is a different issue. A passport is an identity, a travel document, so it's more similar to the identity cards.

And then there is also the fact that some people might not have a particular type of card. They might not have a driver's license. I have colleagues, diplomats, who do not drive their own cars. They do not have a driver's license. So what do you do with those people if you would—in Belgium, if you would generalize the driver's license to be used instead of an identity? You would then have to find a system where you would issue driver's license with no rights to drive a car, for identification purposes, which is not really what it's about. So that is one thing.

We have a feeling in Belgium that the inappropriate use of other identifiers affects the highly sensitive civil liberties issue, because you'd be abusing other cards and information contained in those cards in other systems; abuse of this information for just mere qualification and identification.

What would also disappear if you would take away this card—and this is probably typical for Belgium and not for a country like the United States—is that it's very convenient for people. We can travel in Europe with the ID. We do not need passports to travel in Europe to countries like Turkey or other neighboring countries. We have agreements there. So if we would abolish the card in Belgium, many more people would need passports, and this would increase the costs, as well, for those people as for the administration to issue all these extra passports.

In the case of police checks, if something happens and people are stopped in the street, in the car or whatever, the fact that we have the identity cards and a very efficient data base does save a lot of time. People can be released after only 2 minutes, just checking if this person is really who he is. So it's also a method there, in our view of civil liberty, that we can release people immediately if there is no need to keep them. We do not need to take them to the office, to the police office.

Another very convenient use of the card is the case of unfortunate accidents. When there is an accident with a person on a bicycle and he carries his card, it's very easy to identify him, to warn his family members. So it's also in the advantage of the citizens of Belgium that the card exists.

And then alternatively, we also quite generally use identity cards to fight credit card fraud in Belgium. In many shops when you would want to pay with a credit card, you would want to need to show your identity card and—the way you would show your driver's license. Thank you.

Mr. HORN. Thank you very much.

[The prepared statement of Mr. Veestraeten follows:]

Identity Cards and National Register in Belgium

1. History of the Belgian Identity Card

Belgium has a longstanding practice of registering its citizens.

In 1856, a law was adopted by the Belgian Parliament organizing for the first time the registration of all inhabitants with the local authorities. All cities, towns and villages had to open a register and keep track of people's addresses and the composition of their families. In the 19th century, there was no document issued as a proof of registration. The only individual documents known then were a passport, for use by international travellers.

The German occupation force introduced for the first time an identity card, between 1914 and 1918. This German card was essentially introduced for police and military purposes. However, since there existed already a registration process in Belgium, this new practice did not bring negative reactions as such among the population.

Based upon this experience and convinced of the usefulness of the introduction of an identity card for civil purposes, for ease of identification and for security reasons, the Belgian Parliament generalized the use of an identity card in 1919.

Originally, this card was issued at the moment of the registration with a local authority. It contained 3 parts and a passport sized picture.

Later on, the size and view of the card was modified several times. Security features have been added, especially since in the 60's and 70's, with the increase of organized crime events, the identity card had proven to be easy to counterfeit.

2. FACTS ABOUT THE BELGIAN IDENTITY CARD

The current card was introduced in 1985. It contains an integrated passport sized picture and many security features such as microprint, a hologram, special fonts, refined watermarks and the more. The card is sealed in plastic. It measures roughly 4 by 3 inch (7 x 10 cm). It is usually issued for a period of 10 years, except for children 5 years.

The Belgian identity card contains the following data on the front side:

- Name and first name
- Nationality
- Date and place of birth
- Mention male/female
- Signature of the bearer
- Address
- Card number
- Date of issuance
- Valid until (date)

The card bears a sticker on the back side. On this sticker are mentioned some additional data, if the bearer wishes to do so:

- Card number (for security purposes)
- Marital status and name of spouse
- Number of the National Register

This extra information can only be mentioned upon explicit approval by the bearer of the card. Most Belgians do not oppose these mentions, but they have a right to do so.

The identity card does not contain a machine readable zone today; the insertion of a scan able code is foreseen for the near future.

The card is automatically issued to every Belgian citizen over 12 years of age; every Belgian over 15 years of age has the obligation to carry it at all times, while walking, driving a car or riding a bus.

The card is mostly used for genuine identification purposes, such as: banking business, billing information, rental agreements and the more. It is also to be shown to prove sufficient age when a person wants to buy or consume alcohol, buy cigarettes or enter to any area reserved for adults only.

A police officer can ask to see the identity card of any person found in a public space. Although such request on behalf of a law enforcement agency does not need to be motivated, it mostly occurs only when there is a particular reason for a police officer to do so (suspicious behavior, events, security reasons).

The identity card also permits Belgian citizens to travel to a number of countries without the need for a passport. The list of countries include all Western European countries as well as Turkey, Hungary, Croatia etc. The facility to travel with the sole identity card saves time and money to card holders.

3. HISTORY OF THE BELGIAN REGISTRATION PROCESS

After the introduction, in 1856, of the registration with the local authorities and the introduction and refinement, since 1919, of the identity card, the Belgian Parliament felt the need, in the 70's, to improve data management for official purposes.

The identity card does only contain a limited number of data (and the mention of some of them is not obligatory as explained above). The local register, at the city hall, is not easily accessible for other authorities such as the Federal Government, law enforcement agents in the field (and after regular office hours) and Embassies and Consulates of Belgium abroad. It was equally felt necessary for the organisation of fair elections throughout the country that every single person was identified and not counted double. Most of this could only be assured through a unique and central register, in addition to the still maintained local authorities registers.

Because of all these reasons, a new law was adopted on August 8, 1983 creating the Belgian National Register.

4. Facts about the Belgian National Register

The Register is a data processing system which ensures the registration, recording and transmission between authorized public agencies of information pertaining to the identification of individuals. The National Register also harmonizes and centralizes the manner in which these public records on individuals are kept.

Under this system, every Belgian citizen is given an identification number when he or she is registered in the National Register. This number allows the municipal authorities, diplomatic or consular post or law enforcement agencies to access several records of the individual (data about the identity, driver's license, passport, military service, country of origin, marital status, successive addresses in Belgium and abroad, etc).

The protection of privacy is guaranteed by law. All those who handle the data are bound to keep it confidential. Each individual may see the records kept about him or her and may demand a correction of any errors they may contain.

The Register contains information about both Belgian citizens, residing in Belgium or abroad, and non Belgians residing in the Kingdom.
For every person with a record in the Register, the following data are legally required to be mentioned as a minimum and if applicable: 1) name and first name, 2) place and date of birth, 3)male/female, 4) nationality, 5) main residence, 6) place and date of death, 7) profession, 8) marital status and 9) composition of the family.

In addition to these minimal data, the register also contains: passport issuance data (passport number, date of issuance and expiration), driver's license data, identity card data, successive addresses (in Belgium and abroad) throughout one's life, a chronology of family composition and marital status (mariage, divorce, adoption). Access to these additional data is regulated amd limited to what a particular authority would really need to know and see.

Only the persons mentioned in the law have access to the data gathered in the Register. Such persons include: the Minister in charge of Immigration Policy (and his delegates), the civil servants in charge of registering motor vehicles, the Commander of Police, the Magistrats of the Courts of Justice, the local authorities, etc.

These same persons are held responsible by law for the confidentiality of the information available to them, as well as entered into the system by them. The law is very explicit about the requirements: data must be kept secret; erroneous mentions must be corrected; available information must be entered into the system; no information can be altered without due documentation; any problem with software or hardware must be mentioned immediately. Sanctions for breaches to these rules include stiff fines and prison sentences ranging between 8 days and 5 years.

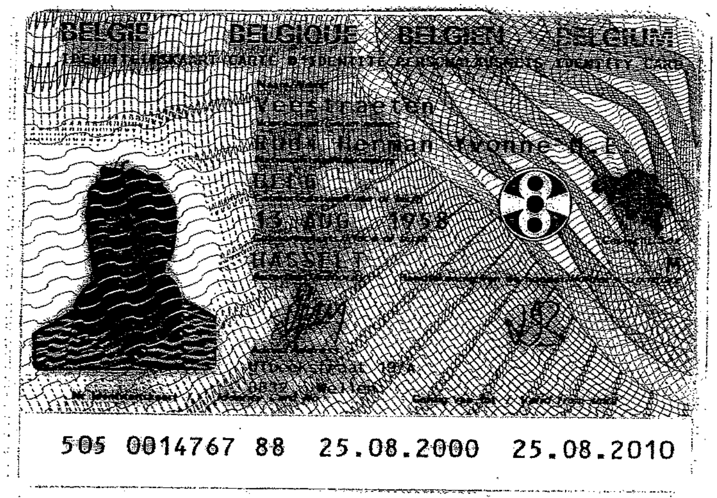
5. FUTURE OF IDENTITY CARD AND NATIONAL REGISTER

The Belgian Government prepares a new faze in the automation and centralization of data management.

The new generation of identity card will allow citizens to make better use of the public service in Belgium. It will allow for the era of e-government.

Access to e-government services will be set up with an enhanced identity card, possibly credit card sized, with a built-in computer chip for automatic identification on the web. This will make it possible to obtain a birth, marriage of death certificate from one's home desktop computer, after due registration and identification through the identity card. Likewise, better security can be assured in banking or other business.

A person registered will much more easily be able to check the data available in the system and to have any erroneous information corrected immediately. This might even incease public acceptance of the system, although this has seldom been a problem in Belgium in the past.



BELGIE BELGIQUE BELGIEN BELGIUM

IDENTITEITSKAART CARTE D'IDENTITE PERSONALAUSWEIS IDENTITY CARD

Verstraeten

Rudi Herman Yvonne H.E

BELG

13 AUG. 1958

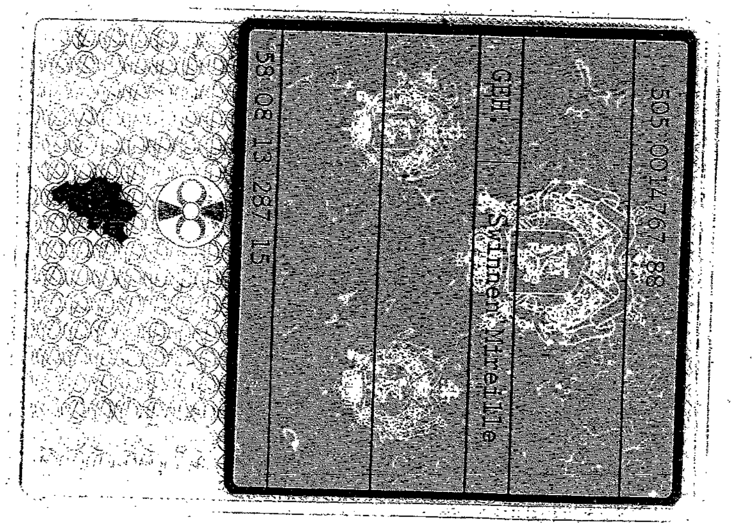
HASSELT

M

Wibostraat 19A

3832 Wellen

505 0014767 88 25.08.2000 25.08.2010



505 0014767 88

GEH. Swinnen Mireille

58 08 13 287 15

Mr. HORN. We're going to recess now because we have to get through the testimony, and I want to give them full rein, Mr. Hoechst, Mr. Shneiderman. So we're in recess until 12:45; in other words, quarter of 1. We have a motion on the floor to recommit with instructions and a passage situation. So we're in recess until 12:45.

[Recess.]

Mr. HORN. The subcommittee will be in order and the recess is adjourned, and we will start with Mr. Veestraeten, who might not have been completely finished; so you're certainly welcome if you want to give a few sentences.

Mr. VEESTRAETEN. Yes, sir, I was finished. Thank you so much.

Mr. HORN. OK. We will then move to Mr. Hoechst, senior vice president of technology, the Oracle Corp. Thank you for coming.

Mr. HOECHST. Thank you, Mr. Chairman, Representative Schakowsky, and members of the subcommittee. On behalf of Oracle, I would like to thank you for inviting me to participate in this discussion. I would also ask that my comments and written testimony be submitted to the record, along with an article written by our CEO, Larry Ellison——

Mr. HORN. Without objection, that will be in.

Mr. HOECHST. Thank you. The reason I ask to do that in particular is the article in its original form makes arguments about this issue that eventually were culled out during the endless number of editing processes that go on as the articles reach sound bites. And so I think many of the issues that are relevant to this discussion, which I'll address in my comments, were part of that original proposal as well.

As we know, information is an incredibly powerful tool, and whether we're using it to make decisions in a boardroom or on a battlefield, whoever knows the most about their situation is the most well prepared to make competent decisions. And in the country today, whether we're in the government system or in the private sector we have countless data bases with all sorts of information being gathered as part of the everyday processes of modern life. And the challenges associated with providing broader access to this information is exactly what we've been working on for the last several years, but the reality is that knowledge which is culled from these data bases is not about the data itself, it's about the relationships that exist between data. And as was fairly thoroughly discussed, I think, in the prior panel, in our opinion the real challenge is not creating new data bases based on these various systems; it is coming up with a standard and secure a consistent means of establishing relationships between these data bases when it's relevant, sharing information across these organizations, whether they reside within a single agency or across agencies or even into the private sector.

So when we talk about a national ID card, I really think what's important to remember is it's not about the card. The card may—we'll see in my comments in a few minutes—may have some interesting capabilities to make the process of securing our systems more convenient and more straightforward. But what we really want to focus on is the relationships between critical information systems. And in the example that was brought up earlier regarding what was sort of known about the people before September, the terrorists involved with the events of September 11th, before the fact versus after the fact point readily to this point.

After September 11th the FBI was able to discover a great deal about the people that were part of this act. The challenge was not that data did not exist. We know the data existed, because we know they gathered it after the fact. The point was that we were unable to establish relationships between those pieces of information to make competent decisions.

Now, we can make decisions after the fact, but this is the difference between investigation and prevention. And so if we are able to address the idea that through a common way of identifying people inside information systems and standards for sharing that information between systems is adopted, then we have a much greater opportunity of taking advantage of all the information that we're already collecting when it can still be used to make a difference.

Now, if we think about the technical approaches with consolidating data bases in this fashion, there's lots of different things we can do. First is the idea of consolidation. We could start to bring together information systems from various organizations even inside agencies or, more importantly, across agencies, into huge monolithic government-managed data bases of everything we know about people. This is not only a poor idea, it's not possible. Whether it's technically possible aside, it's socially not possible. The inertia that exists in information systems and inside organizations, and overcoming the challenges of getting those organizations to roll up their information into systems that they don't control is really a task that would be very difficult to accomplish. Not to mention the fact that the government ought not to be in the business of building huge consolidated data bases of information about people.

Instead, we could decide that it's more important to keep these information systems separate and let them do what it is they do today—and they are already, like we said, gathering all sorts of information—but create some standard ways for them to share that information with one another, and this could very reasonably be aided by a common identifier of people. So if we said between system A and between system B, whether that's immigration and FBI or an airliner, airline company and FBI, to validate that we're both talking about the same person—having standards for doing that could be very helpful in making that sort of communication more facile.

There are also other approaches which are not full consolidation or full distribution and connectivity, and this comes in the flavor of what I call sort of consolidated indexes of information. So, for example, when a police officer pulls over a speeding motorist and wants to check for outstanding arrest warrants, does it make sense for that officer's system to check every local and State law enforcement agency in the country, in real time, to discover whether there are outstanding arrest warrants? Of course not.

Maybe it would be prudent for us to have a national system that points to outstanding arrest warrants; again, the government not managing them, but the government providing a more convenient way of checking across systems that really do the same thing. And, in fact, the Department of Justice has implemented just such a system for that problem.

So the reality is all sorts of these approaches, when we talk about the consolidation and sharing of information, will be part of the ultimate solution. We will have the opportunity to consolidate systems that currently are duplicating efforts. We'll have the opportunity to teach systems that don't communicate with one another to do just that. And we'll have the opportunity to create hybrids, assuming of course that we come up with some standard methods for doing that.

The challenges in this fall into two buckets. First, the technical challenges. The real challenge with an identification system like this is not just relating to people and to information systems, it is associating a human being with a given identity. How do I determine that this person standing in front of me is the same person I'm talking about inside this information system or collection of information systems? And that identity comes through many of the ideas discussed today. It may be in the form of a card. It may be in the form of biometrics, creating a secure and consistent biometrically enabled identification card that anyone could use to establish, to authenticate identity would be very difficult. Not only difficult socially, but difficult technically. The state-of-the-art here is advancing, but it needs to advance further before we could turn such a system on in short-term.

However, there is great opportunity for us to take incremental steps when attacking the technical challenges. First, in establishing standards for national identity, an identifier that uniquely identifies people and government, guidance that should be used when building information systems related to these issues could be done incrementally and systems could come on line as they choose to start to exploit such an identifier.

We also talk about making the existing identification cards stronger rather than trying to establish a new one, and there I think that the driver's license is a good candidate for that because we've seen a lot of work already done there.

And then finally, in introducing specific populations to this technology, rather than saying everyone has to participate, maybe we first focus just on critical jobs; people, for example, whose job requires that they are on the tarmac in an airport, or specific populations of people, be it non-citizens visiting the country, for example.

From the technical perspective of a technology company and representative of that, I would like to suggest that with the competent use of existing technology, we can improve the security not only of identifying individuals but of establishing relationships between information systems that already exist today.

On the social side it's not so clear. And as the debates have gone on today, the issues related with privacy and the whole idea that the government is getting into the gathering and establishing of large centralized data bases is an important debate. But honestly, I believe that it comes down to the difference between: Can we do something and should we do something? The ability to do this and strengthen security is there. The decision as to when this should be done falls in the hands of policymakers like yourselves.

It's important to remember that a discussion of whether we should do that has to be built on top of the ability to say that we can do that and—but for that "should" particular part of the debate, I think it's most appropriate to leave it to policymakers to draw those lines of when such a system should be exploited.

So, given that, I appreciate your time and your opportunity to let us comment in this debate. Thank you.

Mr. HORN. Thank you.

[The prepared statement of Mr. Hoechst follows:]

Statement of

Tim Hoescht
Senior Vice President
Technology
Oracle Service Industries

Before the

Subcommittee on Government Efficiency, Fiancial Management,
and Intergovernmental Relations
Committee on Government Reform
United States House of Representatives

16 November 2001

Mr. Chairman, Vice-Chairman Lewis, Representative Schakowsky, and distinguished members of the Subcommittee, on behalf of Oracle , I would like to thank you for inviting me to participate in this discussion.

Information is one of the most powerful tools that we have at our disposal. Whether we make decisions in a boardroom or on a battlefield, the more we know about our situation, the more effective we can be.

Today it seems that we have countless information systems. Throughout government and industry we keep track of every fact and figure used in the processes of modern life. We've been working very hard for the last few years at making the data in these systems more available to the people who need it. The reality is, however, that having access to these databases alone is not enough to support our critical decision making processes. Real information isn't about data, it's about the relationships between data. Often, the most profound insights are derived only when facts from totally separate systems come together.

There's been a lot of discussion about creating a national ID card. It's my believe that what's most important about today's discussion is not the card itself, but rather the relationships between critical information systems that a standard identifier will enable.

Throughout the United States, we have innumerable systems that include information about all of us. Whether it's banking transactions, telephone calls, arrest warrants, driving records, retail purchases, flight reservations, or terrorist watch lists –they are all associated with someone. The difficulty is that all of these systems use different methods to identify individuals and there is no consistent, reliable, and secure way to relate people across these systems. In order to know that a person who purchased an airline ticket is the same person who is on a terrorist watch list, the system that tracks airline purchases, and the system that tracks terrorists must use the same method of identifying people.

By establishing a standard and secure national identifier, we could ensure that any system that chose to use it could effectively share information with others systems that use it.

Once we have a common identifier that allows us to relate data, there are several different approaches to creating a useful integrated system. At one extreme, for example, we could build one, huge, consolidated database that contains everything we know about a person. Even if we decided for some reason that this was a good idea, it simply isn't going to happen. Any technical challenges aside, the social complexities of getting organizations to share their data in this fashion are fundamentally insurmountable. There are also difficult privacy and security issues involved with co-mingling data of various sensitivities.

The reality is that all of our systems will continue to remain separate. The goal is to accept this reality, and teach these separate systems to ask each other questions when it is relevant. For example, an airline system could ask a law enforcement system if someone is permitted on an aircraft. Of course, the airline system and the law enforcement system will remain separate, but by simply checking with one another, a crisis could be avoided. This is the difference between investigation and prevention. Many important relationships can already be established today through time-consuming research, but this is often too late to be of use. We saw after September 11th, that the FBI was able to find out that we had all sorts of information about many of the terrorists. We were not, however, able to get this information when it was most needed: when they entered the country, when they took flying lessons, or when they boarded the aircraft. We're not talking about creating any new data sources, we're just talking about making the existing data sources useful before the fact, rather than after it.

Of course, there are also hybrid approaches where the systems are separate but they "publish" small subsets of information to central warehouses (with pointers back to the details). For example, when a policeman pulls over a speeding motorist, he may want to check for any outstanding arrest warrants. Is it practical for his system to check with every state and local law enforcement system in real time? No. Instead a single, national database of arrest warrants makes such a check more realistic. In fact, the Department of Justice has created just such a system.

In reality, all of these approaches will be used in various situations. But, regardless of the granularity of these systems, the common identifier makes it possible to establish these important relationships.

Now, assuming the federal government is prepared to move in this direction, there are great many technical and social challenges. Technically, creating the standard identifier is the easy part. We could even use an existing one such as Social Security number. But building a secure and reliable way of establishing the identity of individual human beings is much more difficult. This is where the ID card comes in. Combined with biometric technologies, it offers the potential to assign to each person a means of uniquely identifying themselves to an information system. Creating a card that is difficult to forge and that consistently and uniquely identifies an individual person is clearly not an easy problem. The technologies that would support this are maturing quickly despite the fact that they have not been a priority in industry R&D budgets.

The most practical approach to addressing the technical challenges is an incremental one. First, systems can, one by one, begin to use the national identifier. When they are ready, they can participate. Second, rather than creating yet another card infrastructure, the federal government, working with state and local governments, could incrementally evolve one of the existing ID cards -- the driver's license being the most likely candidate. And third, instead of telling everyone tomorrow that they need an ID, government could start with critical jobs (like pilots or anyone who works on the tarmac at an airport), and key populations, such as noncitizen residents or those here on a work or tourist visa. Then, over time, we can broaden it to include other key populations.

What is clear is that, technically, we could improve the security and reliability of the existing infrastructure.

Socially, it's not so clear. The primary concern here is one of privacy. People who fear a system like this don't want information about themselves in these databases. We're well past this fear being remotely consistent with reality. If you buy things, or make phone calls, or drive a car, or commit crimes, or fly, or leave the country, or go to the doctor, you actions already are being gathered and stored. Some of these systems are government systems, but most of them are in industry. In many cases, others can even purchase this information from the companies that collect it. A national ID that is managed by the government doesn't mean that the government is in the business of collecting information, it simply means that it is in the business of certifying identity.

Having such an ID also doesn't mean that it'll be a free-for-all of systems access. Just because the FBI chooses to use a national identifier to track people doesn't mean that anyone is allowed to access their systems. Nor does it mean that the FBI is allowed to access every system that uses the ID. Such access will be regulated by policymakers just as is it today. Policymakers may decide that it is appropriate for airlines to check if a passenger is on a terrorist watch list but that it's not okay for them to check whether they have unpaid parking tickets.

It comes down to the difference between "can" and "should." Can we create a standard means of securely identifying people and sharing information about them between systems? Yes, I believe so. Should we use such a system to increase security in the United States? That is the question has fallen upon members of Congress. Remember, though, debating whether we "should" is irrelevant without discussing whether we "can" institute the technology.

Thank you again, Mr. Chairman, for the opportunity to appear before the Subcommittee today, and I look forward to answering any questions you may have.

Life, Liberty and the Pursuit of Terrorists

by

Larry Ellison
Founder, CEO
Oracle Corporation

Francis Fukuyama, the former State Department official who authored the essay "The End of History," stoutly declared in the aftermath of the terrorist attack of September 11th, "We are an open society, we will not resort to ID checks." He is quite correct that many Americans instinctively fear that a national ID card would sacrifice basic freedoms and compromise personal privacy without contributing to a reduction in terrorism. They suspect that our government would build Big Brother databases that would be better at snooping on law-abiding citizens than catching terrorists. Few would disagree that if we do indeed lose our liberty the terrorists will have won.

Issuing ID cards to American citizens and visitors to the United States seems, on the face of it, like a very big deal. Surely trusting government to maintain a database with our names, addresses, places of work, amounts and sources of income, assets, purchases and subscriptions, travel destinations, and so on, requires a huge leap of faith? Gathering information about American citizens is not the business of government; it's the business of American Express and Visa. For years they've been issuing cards and building massive databases on millions of American citizens. These databases are searched and sold on a daily basis. It turns out that most of us have voluntarily bartered away our essential liberties and personal privacy to make shopping more convenient.

Since credit card companies already issue cards and maintain databases on us, why shouldn't government be allowed to do the same thing? That's missing the point. The government already issues several ID cards: social security cards, driver's licenses, pilot's licenses, passports, visas and so on. The government also maintains thousands of databases in an effort to keep track of virtually everyone, from taxpayers and registered voters to suspected terrorists. The question is not whether the government should issue ID cards and maintain databases. The question is can the ones we have be made more effective, especially when it comes to keeping tabs on potential terrorists.

Do we need a national ID card? No. Should we make our existing ID cards harder to forge? Yes. Do we need more databases to track terrorists? No, just the opposite. A very large part of the problem today is that we have too many. The single greatest step we could take to making life tougher for the terrorists would be to ensure that all the information in myriad government databases was copied into a single, comprehensive national security database.

Today, every federal intelligence and law enforcement agency - the CIA, the FBI, the INS, the NSA, not to mention all manner of state and local bodies - maintain their own separate databases on people suspected of being criminals or terrorists. There are lots of agencies, so there are lots of databases. Unfortunately, a multitude of separate databases makes it very difficult for one agency to know about and apprehend someone wanted by another agency.

That's why one of the terrorists made it through passport control, even though he had an outstanding arrest warrant in Broward County, Florida. The FBI was searching the country for a couple of others because CIA intelligence revealed that they had ties to Osama bin Laden. Four more were sought by the Immigration and Naturalization Service because they were in the country illegally. Unfortunately, it's pretty easy to escape detection once you're in the country because the federal watch list is very rarely cross-checked.

When the airlines sell tickets the names of the passengers are not cross-checked with names on the watch list. If this database cross-checking had been done, many of the terrorists would have been caught before they boarded their flights. Mandatory cross-checking could be supplemented with various voluntary checks. Companies concerned about security might elect to submit the names of potential employees as a part of their reference checking process. If the submitted name was on the watch list the company would not be notified, but the FBI would be. The FBI could then opt to put that person under surveillance or under arrest.

Another challenge is tracking people with multiple or stolen identities. The good news here is that a national security database combined with biometrics, thumb prints, hand prints, iris scans, or whatever is best, can be used to detect people with false identities. To gain entry into an airport, or any other secure location, would require someone to present a photo ID, such as a current driver's license, put their thumb on a fingerprint scanner and tell the guard their social security number. The name and social security number are then keyed in and sent, along with the digitized thumb print, to the national security database.

An ID card storing a digitized version of your name and address would make airport security check-in more convenient. Insert your card, put your thumb on the scanner; the database cross-check is done, and you're through in a few seconds. The digital ID can be based on current credit card technology, which is much harder to counterfeit than most driver's licenses, or on smart card technology, which is even better but more expensive.

There is no need to compel any American to have a digital ID. Some Americans may choose to apply for a digital ID card to speed the airport security check-in process. Some states might select digital IDs for their next generation of driver's license. Credit card companies might also embrace the digital ID standard and automatic biometric checking to reduce credit card fraud. A voluntary system of standardized digital IDs issued by government agencies and private companies could actually prove more effective than a mandatory system.

Stripped of their multiple and stolen identities terrorists become much easier to track using conventional methods that rely on patient, old-fashioned intelligence gathering. Nothing can take the place of that. Unfortunately, over the years we have found countless ways to inhibit our intelligence and law enforcement agencies from doing their jobs. We've been so busy protecting ourselves from our government that we have made it almost impossible for our government to protect us.

We don't need to trade our liberties for our lives. By law, Fourth Amendment protections against unreasonable search and seizure would govern access to the national security database. The "probable cause" standard will still have to be met. With proper safeguards, the only "right" we would have to surrender is that to multiple secret identities.

Two hundred years ago, Thomas Jefferson warned us that our liberties were at risk unless we exercised "eternal vigilance." Jefferson lived in an age of aristocrats and monarchs. We live in a nuclear age with the threat of terrorists getting their hands on weapons with the capacity to destroy entire cities. Only by giving our intelligence and law enforcement agencies better tools and more latitude to pursue terrorists can we expect to save life and liberty together.

The author, Larry Ellison, is the founder and CEO of Oracle Corporation, the world's largest supplier of database technology. Oracle's first customer was the CIA. Mr. Ellison has offered to provide the software needed to establish a United States national security database without charge.

Mr. HORN. And our last presenter is Dr. Ben Shneiderman, professor, Department of Computer Science, University of Maryland at College Park; and he is also here as a fellow, on behalf of the Association for Computing Machinery. Thanks for coming.

Mr. SHNEIDERMAN. Thank you, Chairman Horn, for the opportunity to testify at this timely and important hearing. I want to commend you, Ranking Member Schakowsky, the subcommittee members and your staff, for turning Congress's attention to proposals for a national identity card system. You've given some of my introduction already, and I will say for further purposes that my statement represents the Association of Computing Machinery's Committee on U.S. Public Policy.

The ACM is a nonprofit educational and scientific society of 75,000 computer scientists, educators, and other competing professionals from around the world, committed to the open interchange of information. In the 2 months since the deplorable acts of terror were perpetrated against America, a number of legislative measures and regulatory actions intended to ensure the safety and security of our citizens have been proposed. While most proposals have been well intentioned, some have been misguided in that they overlook the potential for unintended consequences or underestimate the technical challenges and risks inherent in their implementation.

Recently, information technology vendors have suggested that a comprehensive national identity card system could be created and implemented in as little as 90 days. Implementing such a complex system is a challenging systems engineering matter. Such a rapid construction of an effective and novel socio-technical system would be unprecedented. A constructive alternative may be focused efforts that build on existing systems such as State motor vehicle passports and visas. And as the last speaker, I have the luxury of being able to resonate with the many thoughtful comments that have been made already.

The first panel made very clear the strong political concerns about a national system, and this panel has gone through in good detail about some of the challenges in the technical development. A national ID system requires a complex integration of social and technical systems. That's what I'm going to stress here is that combination, including humans to enter and verify data, plus hardware and software networks to store and transmit.

Such socio-technical systems are always vulnerable to error, breakdown, sabotage, and destruction by natural events for any people with malicious intentions. For this reason, the creation of a single system of identification could unintentionally result in degrading the overall safety and security of our Nation because of unrealistic trust in the efficacy of the technology.

The National ID card itself is only the most visible component of a system that would require supporting bureaucracies and elaborate data bases that would have to operate in everyday situations; again, as said by several members of this panel. In particular, a national ID system requires an extensive data base of personal information of every citizen. Who would enter the data? Who would update it? Who would verify it? Who would determine when the data is no longer trustworthy? Who would review audit trails and approve access?

If a new and centralized approach is technically problematic, as again has been stated by many, and politically unpalatable, which seems quite well accepted here, then how might we work to increase security? Constructive first steps would be to define goals and develop the metrics of success. Let me repeat that. Constructive first steps would be to define our goals in a narrowly focused way, and develop the metrics of success. If improved air travel safety is our goal, and it has wide public support, then we need to develop the techniques to achieve that goal, with modest impact on personal rights and privacy. A realistic goal would be to make verifications of passenger identity more reliable, while limiting delay, intrusion, and inconvenience to citizens.

Improving State motor vehicle identification cards might be accomplished by coordination among the States to determine best practices for issuing, replacing, verifying, and monitoring usage. Such efforts might be coordinated by the National Association of State Chief Information Officers, as mentioned by Newt Gringrich, or by the National Governors Association. Common practices or even national standards might be arrived at through public discussion. Adequate public discussion of proposals is essential to gain acceptance and to improve their quality.

A socio-technical systems approach would include quantification of weaknesses and vulnerabilities of data base security and network access based on existing systems. Then realistic solutions to dealing with problems such as lost cards and mistaken identifications would have to be developed and tested. Special cases such as tourists, professional visitors, foreign students would have to be addressed. Any complex social technical system such as identity verification requires well-trained personnel whose performance is monitored regularly. Effective hiring and screening practices, chances to upgrade their skills, and especially participation in the redesign of the system, are important contributors to success.

Improvements for citizens could also lead to higher data reliability and system efficacy. Citizen confidence and data accuracy could be improved by system designs that provide greater transparency and greater openness, by allowing citizens themselves to inspect their contents and view a log of who uses their data.

More constructive ideas could emerge by encouraging research by computer and information scientists in collaboration with social scientists. They would also be encouraged to build bridges with legal and policy groups so that their solutions are realistic and implementable.

It's important that the Congress proceed cautiously on the issue of national identity card systems. They involve risks and a variety of practical organizational and technical challenges. Any effort to improve homeland security should begin with clear statements of goals and quantifiable metrics of success. Computer technology can do much, but it cannot see into the minds and hearts of people, nor can it replace the capability of vigilant citizens.

Face-to-face security checks must be a vital component of airport and other security systems. On this point I also differ from Mr. Goodman's report about Ben-Gurion Airport, where it is not a biometric system, but it is repeated face-to-face encounters with security checkers who ask questions and are vigilant to the responses and the behavior of each person passing through that airport, as I did late in August of this year.

Despite growing public and political pressures from perceived security enhancements, the risks and challenges associated with a national ID card system need to be identified and understood before attempting deployment. The problems cannot be solved overnight or in 90 days, as has been suggested, but constructive alternatives such as improving existing State motor vehicle registration and passports are promising possibilities that could bring benefits sooner than establishing an entirely new system. The emphasis must be on people first, then the technology.

The Association for Computing Machinery and other leaders in the computing community are ready and willing to assist lawmakers in their efforts to enhance the safety and security of our Nation.

Thank you for the opportunity to speak here.

[The prepared statement of Mr. Shneiderman follows:]

Testimony to:

House Committee on Government Reform
Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations

From: U.S. Public Policy Committee (USACM) of the Association for Computing Machinery (ACM)

By: Prof. Ben Shneiderman, University of Maryland

National Identification Card Systems

November 16, 2001

Thank you Chairman Horn for the opportunity to testify at this timely and important hearing. I want to commend you, Ranking Member Schakowsky, the Subcommittee members, and your staff for turning the attention of Congress to today's discussion regarding proposals for a National Identity card system.

By way of introduction, I am Ben Shneiderman, a Professor in the Department of Computer Science at the University of Maryland at College Park. In addition, I am Founding Director of the Human-Computer Interaction Laboratory, and Member of the Institute for Advanced Computer Studies and the Institute for Systems Research at the University of Maryland. I am a Fellow of the Association for Computing Machinery and a Fellow of the American Association for the Advancement of Science.

This statement represents the Association for Computing Machinery's (ACM) Committee on U.S. Public Policy (USACM). ACM is a non-profit educational and scientific computing society of 75,000 computer scientists, educators, and other computer professionals committed to the open interchange of information concerning computing and related disciplines. The Committee on U.S. Public Policy acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. It seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community.

Introduction

In the two months since the deplorable acts of terror were perpetrated against America, a number of legislative measures and regulatory actions intended to ensure the safety and security of our citizens have been proposed. While most proposals have been well intentioned, some have been misguided in that they overlook the potential for unintended consequences or underestimate the technical challenges and risks inherent in their implementation.

Recently, information technology vendors have suggested that a comprehensive National Identity card system could be created and implemented in as little as 90 days. Implementing such a complex system is a challenging system engineering matter. Such rapid construction of an effective and novel socio-technical system would be unprecedented. A constructive alternative may be focused efforts that build on existing systems such as state motor vehicle identification and passports.

Practical Concerns

From a practical standpoint, a National Identity card system would not have prevented the tragic terrorist acts of September 11. Evidence suggests the suspected hijackers made no effort to conceal their identities. In fact, several of the suspected terrorists possessed state-issued ID cards with their pictures and names.

Proponents of the National Id system suggest that cards will authenticate the identity of individuals. **However, the positive identification of individuals does not equate to trustworthiness or lack of criminal intent.**

The quality of forged public documents is often so good that they are accepted as authentic. According to the Suspicious Activity Reports (SAR) filed by U.S. financial institutions, thousands of counterfeit credit cards have been reported over the last several years. The credit card industry has accepted that losses due to high-quality counterfeit cards are simply a cost of doing business.

As with any system that depends on human and technological components, insider abuse is a risk. Currently, there is no method of ensuring that forgery, bribery, or coercion will not put the proposed form of identification in the possession of those with criminal intent. As the recent Virginia case demonstrates, motor vehicle department employees have issued unauthorized drivers' licenses for financial gain or other personal reasons.

Socio-Technical Challenges

A national ID system requires a complex integration of social and technical systems, including humans to enter and verify data, plus hardware, software and networks to store and transmit. Such socio-technical systems are always vulnerable to error, breakdown, sabotage and destruction by natural events or by people with malicious intentions.

For this reason, the creation of a single system of identification, could unintentionally result in degrading the overall safety and security of our nation, because of unrealistic trust in the efficacy the technology. The National ID card itself is only the most visible component of a system that would require supporting bureaucracies and elaborate databases that would operate in everyday situations. In particular, a National ID system requires an extensive database of personal information on every citizen. Who would enter the data, update it, and verify it. Who would determine when the data is no longer trustworthy? Who would review audit trails and approve access?

We must ask whether there is now a secure database that consists of 300 million individual records that can be accessed in real time? The government agencies which come close are the Internal Revenue Service and the Social Security Administration, neither of which are capable of maintaining a network that is widely accessible and responsive to voluminous queries on a 24 hour by 7 days a week basis.

Can records on everyone in the United States or even all foreign visitors be organized and maintained in one database? Compiling the necessary database to support the system would require a massive data-collection effort beginning with the interconnection of databases held by local, state and national government networks and some private entities. Determining what information to include in the database will no doubt prove to be controversial.

Once the problem of gaining access to the amount of information required is solved, there still would be challenges in creating a system that could communicate with all of the varied computer networks that would house components of individual identification.. The difficulty of communicating with intra-federal, intergovernmental, and private sources of information in real time environment is unprecedented.

An underlying software foundation is required to make the system work. In addressing the problems of building a large enough network and/or creating a workable cross database network communication system, redundancy and backup issues must be addressed. Formulating protocols and procedures for the proper maintenance of databases that are enforceable are part of this technical challenge.

Once the information is gathered, how will the information be transmitted? Who will have access to the information? Will there be limitations on how the information can be used by front line workers?

The next question involves how persons present their identification to those in authority who demand it. Will the identification be a card, with a photo, signature, thumbprint or other identifying biometric? While biometric technology is advancing rapidly, new socio-technical concerns have arisen that need to be addressed before large-scale implementation.

Regardless of the method used to create a new identification tool, the system would require professionally trained staff at specialized terminals at every point at which the National ID card is to be used. Devices like card readers supporting databases and communication complexes would be necessary to support National IDs. An extensive and secure nation-wide communications network to connect multiple terminals to the database would also be required.

Security Risks of the Infrastructure

There are nearly 300 million residents in the United States. To what extent can a national identification system be created that would provide confidentiality, authentication, integrity, access control, and availability to a group of users who are geographically dispersed with an acceptable rate of false positives or negatives?

Confidentiality speaks not only to the issue of privacy, but to the safe transmittal of information over great distances. The current state of the Internet might make it unsuitable for this purpose. Authentication requires that the system must be able to accurately verify the identity of people. Integrity speaks to the high level of trust and acceptance this system must have to be depended upon by security and law enforcement. Access control must be limited to those with proper clearance and authority. This is important if confidentiality, authentication, and integrity are to be maintained.

The technology would have to prevent interruption of communications from natural or man made causes, interception of information by unauthorized parties, unauthorized modification of information stored in networks or while in transit, finally the system would have to insure that fabrication of information was not possible.

As this Subcommittee knows from its computer security efforts, strong system security is presently an unsolved socio-technical problem, even in the most advanced systems. There are a great many problems that need to be addressed to help secure our nation's infrastructure. My colleague Dr. Peter Neumann of SRI has documented the myriad ways that computerized identification systems have been compromised with sometimes devastating results.

Databases are vulnerable to exploitation and attack. A national identification database could provide a new target for malicious computer users. As evidenced by the poor computer security grades awarded last week by this Subcommittee, vandals have routinely corrupted government computer networks. Unauthorized intrustions to the National ID database may use that information as a means to conduct identity theft or to profit by the sale of that information to others with criminal intent.

The disclosure a few years ago that IRS personnel were reading the private tax returns of prominent Americans was unsettling for most of us. A National ID system places an even greater amount of information in reach of those who might abuse it.

Constructive alternatives

If a new and centralized approach is technically problematic and politically unpalatable, then how might we work to increase security. **Constructive first steps would be to define goals and develop metrics of success.** Improved air travel safety would have wide public support, if the techniques to achieve that goal had modest impact on personal rights and privacy. A realistic goal would be to make verifications of passenger identity more reliable, while limiting the delay, intrusion and inconvenience to citizens.

Improving state motor vehicle identification cards might be accomplished by coordination among states to determine best practices for issuing, replacing, verifying, and monitoring usage. Such efforts might be coordinated by the National Association of State Chief Information Officers or the National Governors Association. Common practices or even national standards might be arrived at through public discussion. Adequate public discussion of proposals is essential to gain acceptance and to improve their quality.

A socio-technical systems approach would include quantification of weaknesses and vulnerabilities of the database security and network access, based on existing systems. Then realistic solutions to dealing with problems such as lost cards and mistaken identifications would have to be developed and tested. Special cases, such as people who do not wish to carry a card, tourists, professional visitors, and foreign students would have to be addressed.

Any complex socio-technical system, such as identity verification, requires well trained personnel whose performance is monitored regularly. Effective hiring and screening practices, chances to upgrade their skills, and participation in re-design are important contributors to success.

Improvements for citizens could also lead to higher data reliability and system efficacy. Citizen confidence and data accuracy could be improved by system designs that provide greater transparency by allowing citizens to inspect their contents and view a log of who uses their data.

More constructive ideas could emerge by encouraging research by computer and information scientists in collaboration with social scientists. They should also be encouraged to build bridges with legal and policy groups, so that their solutions are realistic and implementable.

Conclusion

It is important that Congress proceeds cautiously on the issue of a National ID card system. National ID cards involve risks and a variety of practical, organizational, and technical challenges. **Any efforts to improve homeland security should begin with clear statements of goals and quantifiable metrics of success.**

Computer technology can do much but it cannot see into the minds and hearts of people, nor can it replace the capability of vigilant citizens. **Face-to-face security checks must be a vital component of airport and other security systems.**

Despite growing public and political pressures for perceived security enhancements, the risks and challenges associated with a National ID card system need to be identified and understood before attempting deployment. The problems cannot be solved overnight, or in 90 days as has been suggested. Constructive alternatives such as improving existing state motor vehicle registration and passports are promising possibilities that could bring benefits sooner than establishing an entirely new system. **The emphasis must be on people first, then technology.** The Association for Computing Machinery and other leaders in the computing community are ready and willing to assist lawmakers in their efforts to enhance the safety and security of our nation.

For more information about USACM contact Jeff Grove, 202-659-9711, or see the web site http://www.acm.org/usacm

Prof. Ben Shneiderman ben@cs.umd.edu
Dept of Computer Science 1-301-405-2680
Univ of Maryland 1-301-405-6707 fax
College Park, MD 20742
Lab: http://www.cs.umd.edu/hcil Bio: http://www.cs.umd.edu/~ben

Mr. HORN. I have been very enlightened by your presentations. I had a chance to go through them all last night, except for the Senator, who just flew down here, and thank you again.

I just ask all of you, would you object to a form of identification that contained only the person's name and confirmation that he or she is a U.S. citizen? How do you feel about that? That's getting down to essences.

Mr. SHNEIDERMAN. I think the issue is not just the card—again, the card is only the most visible form—but who issues the card, who certifies its correctness, and how it's handled. And my belief and my testimony suggests that strengthening existing systems such as State motor vehicle systems would be the most effective.

We currently have accepted the practice of walking up for airline boarding to show a State motor vehicle card. I think that is the place of intervention where we could do most good to improve its efficacy. Simply creating a new card with whatever's on it I think will lead us down the wrong path.

Mr. HORN. Any thoughts on this, Mr. Hoechst?

Mr. HOECHST. Yeah. I would add that a card that just has a small amount of information, and really even perhaps less than you describe, which can only establish identity, is the only thing that's really feasibly possible to deploy practically. Any attempts to create cards that contain lots of information just opens the troublesome box of discussions about how that information is used. What's important is the information that will be used, once identity is established, is already managed by processes inside organizations, whether they're law enforcement organizations or commercial organizations. What the card only does is to help establish identity, authenticate that this person is this—represents this well-understood and standard identity.

Mr. HORN. Mr. Veestraeten, how do you feel about that; get it down to the name, and are you a U.S. citizen or aren't you?

Mr. VEESTRAETEN. Yes, Mr. Chairman. That is exactly how it is organized in Belgium today. The cards only—I headed a company of—the only cards which I had at hand, which was my own, and with documentation which was disputed, and we only mentioned a limited number of data. This number is limited by law. So nobody can add any additional information. You will see on the back of the cards, there are two items mentioned, and this is on my explicit authorization. I had to sign the documents to approve those mentions. One is the name of my spouse, which I'm happy and proud to have there, and the other one is the number of the national register with this assembled data base, and I also approved in writing to have this item added to my card. If not, it would not have been there. So the only information we add is—we as a standard put on the card: name, first name, date and place of birth, address and nationality. And there is nothing else there.

Mr. HORN. Ms. Corrigan.

Ms. CORRIGAN. I think that in order to answer that question, the Privacy Act, which was enacted in the seventies, was rooted in a golden rule essentially, which is that information collected for one purpose should not be used for another purpose.

And it's difficult to answer your question because information is rarely collected just to collect it. There's usually a reason that you want to have such a list. So, for example, a list of American citizens—and I think you yourself proposed something similar a few years ago—around a voter registry; you know, the difficulty there is, it was the same debate that came up around, No. 1, as Professor Scneiderman pointed out, you know, do we in fact have an accurate list that would reflect that? We do have a passport document when we leave the country, which establishes citizenship obviously? So there are documents that are shown to do that.

Going back to my one of my original points is that to build any one of these data bases on a faulty system of documents is very problematic, particularly when it would deny you either a service or a right that you've got either under law or the Constitution.

Mr. HORN. Senator Goodman.

Mr. GOODMAN. I would like to reiterate once again the notion that in a wartime situation, you have criteria which I think differ materially from those in the halcyon days that we knew before September 11th. And in this instance, the purpose of the card would be to establish clearly and unequivocally the identity of the individual. But let me point out that at that stage of the game, we'd have linkages with various data bases which might ascertain the possible undesirability of that individual's behavior pattern which would require close tracking.

For example, if someone enters the country in a situation where they're here to do mischief, which has all too often in the recent past proven to be the case, it's imperative that we have some means of tracking that individual. To have a society in which everyone can rattle around in a state of happy unanimity, when the assumption that the cool air of freedom must be the thing which we permit them to breathe continuously while we're at war, I think denies the exigencies of the war situation.

Mr. HORN. Professor Turley.

Mr. TURLEY. Well, I suppose I should be delighted with the opportunity to lie about my weight, but I don't think that this is an issue that will be solved by more cards. God knows, Senator Goodman's wallet couldn't hold another one. But I think my problem with it is simply that simply having a card issued on an expedited basis I think puts us on a track of where we've been. That is, there is a natural desire to rush into this room and put this fire out.

But I think it needs more study than that, I think not just because of our traditions, but because we have decided on the technology, its use, its functions, it's appropriate functions. Any dangers of what's called authorized misuse, all those things we have to think about before we plunge into this.

I do think that there is a basis, I say in my written testimony, issue a card relatively quickly for certain insular groups—those may be foreign nationals, they may be foreign students, but they would also be, for example, international truckers—that we do need a very fast system at our borders that's reliable; because we have a buildup at our borders that's going to get worse, particularly during times of crisis. We need to solve that right away and we can create a biometric card to try to do that.

We may also want to use a card; for example, groups that handle material like anthrax. So you can have an immediate card issued.

But what I think we should be careful not to do is to restrict it from drifting, not make it a national card. You focus on those areas we need one right away, and then study the issue of whether we need a national identifier.

Mr. SHNEIDERMAN. Focus systems would be most effective and most prompt, I believe, in producing the benefits that we all seek. But whether it's airport personnel or truckers, we can go—and small groups can be approached and handled in a respectful way.

Mr. HORN. I tried out on our first panel the idea of a commission, which was usually a Presidential commission, of picking the Chair, and then the Speaker of the House, and the Majority Leader of the Senate. And I'm inclined to put that into law and have my colleagues go with it. But what that does is delay things. On the other hand, what it does is try to build a consensus. So we had the Hesburgh one on immigration; we had Barbara Jordan as the Chair, and so forth.

Now, we've been through this in terms of census material, where we wanted to put through a 5-year or so, and they blew it right out because they didn't want any part of it, and it became a jurisdictional argument.

So I'd be interested in what your feeling is. Is it worth getting a commission that has those suggestions of the Speaker of the House and the Majority Leader of the Senate and the Minority Leaders of both houses and the President of the United States? So what do you think?

Mr. GOODMAN. Mr. Chairman, let me respectfully suggest that it does seem to me that approach does take into account the concerns which we feel are increasingly evident, and I'm afraid if we are once again hit with another act of terrorism, which in my judgment is in all probability likely to occur sometime between now and Christmas, it's going to create the same reaction, only on an exacerbated basis, that we had after the World Trade Center and Pentagon episodes. And I must say to you that I think that it's extremely important that we move on with this fairly quickly and try to arrive at a conclusion. I would hope that some form of identification could be established promptly, so that we are protected to the extent possible against a recurrence of this type of an act.

On the lighter side, I'm reminded of the couple at the Atlantic City Boardwalk: The gentleman got on the scale, put a quarter in, and one of those little tickets came out with his fortune on it. And his wife said, "What does it say?" And he said, "It says that I'm a handsome, debonair fellow of extreme brilliance with the highest IQ in Atlantic City." And she said, "Well, let me look at it." And she looked at it and she said, "It got your weight wrong, too."

So that we do have occasional confusions in these mechanical devices, but I think that we're at the point where that type of thing is not likely to occur with any frequency.

Mr. HORN. Ms. Corrigan.

Ms. CORRIGAN. Well, it sounds like the legislation does not have the ACLU chairing the commission, so it would be much easier for us to come out in support of that.

Mr. HORN. Well, we don't know. You're here and——

Ms. CORRIGAN. Hey, I'm available.

Mr. HORN. Yes, and there are minorities in both Chambers.

Ms. CORRIGAN. I mean, I think the key is not whether there is a commission or whether it is staff on a committee developing a legislative proposal. I mean, the question is what's in it and is—you know, the ACLU would oppose an identification system either through the front door of calling it a national ID or through the back door of some other type of registry or integrated data base.

Mr. HORN. Mr. Veestraeten, did Belgium ever have, say, a King's Commission or the Parliament, whatever, to get this moving?

Mr. VEESTRAETEN. No. This dates from long back in our country. So I don't know how it was discussed back in the beginning of the last century, but——

Mr. HORN. And the First World War and the Second World War.

Mr. VEESTRAETEN. The card was introduced after the First World War.

Mr. HORN. Yes.

Mr. VEESTRAETEN. Yes.

Mr. SHNEIDERMAN. I think they have 80 years of history of evolution to develop their approach which fits with their national values. And I think we've got a history of evolution, and I support the idea of a continued evolution to refine existing mechanisms.

Mr. HORN. Mr. Hoechst.

Mr. HOECHST. Mr. Chairman, I would suggest that your concern about a commission—about delaying things, especially with an ID card, that there is an opportunity missed that could be done in the short-term. And so what I would suggest for identification cards, then something that studies it in the form of a commission would be valuable as long as it were given guidance that—along some of the ideas that were proposed today, that it not just study it, but that it is practiced, maybe in prototypical form; giving identification cards to different populations to see how it works, rather than just study it.

But I would also suggest that there is short-term activity that can happen, that I would hate to see a commission cause us not to focus on, and that is on these goals of information sharing, especially between critical information systems in the area of law enforcement and immigration and the like where we do not—the technologies exist. We know they work. We need to choose to use them, and we need to set clear guidelines about when it is appropriate to use them and legal to use them.

Mr. HORN. Thank you. Dr. Shneiderman.

Mr. SHNEIDERMAN. I repeat my desire for the evolutionary, but I think also focused action, as I say, as we heard here; maybe specific interventions between—for information sharing between FBI, CIA. If our concern is aircraft, you know, boarding aircraft, then that kind of sharing of information is a possibility on a very short-term basis.

And then I think focused populations, such as international truck drivers or airport personnel who have access to secure areas, immediate improvements could be made.

But, again, I want to restate it's not just building some technology. It's providing the human infrastructure that builds trust and support for this rather than antipathy. It must be demonstrated that any intervention has broad support, and especially of those who are most directly affected; that it's implemented in a way in which people feel that this does contribute positively, and therefore they are most cooperative with it and they will point out—they'll be vigilant in pointing out those who are potentially in violation.

Mr. HORN. I thank you and yield at least 10 minutes to the ranking member.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman. I think this has been a really important and a very useful hearing. I thank all the panel members. These are questions that we are going to have to seriously consider.

I want to first play a kind of devil's advocate and—because my proclivity is to be—as those of you who have heard my opening statement—is to be very, very skeptical of the notion of a national identification card. But the point that Mr. Veestraeten said, which is that we use identity cards, and all of you—we do that when you go on an airplane, when you cash a check, all kinds of places where we are asked and required to produce some sort of identification. It seems to me if the technology is available to improve on those systems, maybe not perfectly, but to improve on those systems. Then he asked the question or at least made the statement that since we do that anyway, why not have a universal card, a national card.

So, Dr. Shneiderman.

Mr. SHNEIDERMAN. Again, I think the supportive participation from citizens is necessary. If they see this as a universal card collected by a Federal agency, I think the resentment may—and the doubt and the questions, the interference with privacy would be very much in their mind, so you'd have a poor participation and, I think, disruption. People would be concerned.

Whereas, if they apply for their State motor vehicle license, where they recognize that the benefit is they're receiving a card which enables them to drive, that it possibly takes care of health problems should they have an accident, and that there may be other specified focused, clear benefits to it, they will cooperate, and that those who take the information will have a clear sense of purpose and work as best as they can to ensure that the quality of the data is high and that customer satisfaction is high and that participation is broad. And, again, when someone is attempting to forge or bypass the system, there's likely to be stronger citizen participation in stopping such interventions.

I think we have the interesting examples of computer viruses. Why is it that the Lenox communities or the Mack communities have less of this. There's a warm sense of participation. There's an active sense of pride. It's close to them. And so I think if we follow those models and we want to bring, as in this country, we have a long history of bringing things closer to people by having the States be the closest point of connection for such activities, we will be building the right kind of system. And thinking about the social dynamics of why someone offers their information and why they might try to deceive and how they might help to prevent others from deceiving, that's where we will go to build the strongest possible system. So again a diversified system and again a focused one that deals with special communities.

Ms. CORRIGAN. I think here, whether it's a State level document like the driver's license or a Social Security number or a newly issued type of identifier like the biometrics, I think we have to go back to the purpose for which we are gathering this information. And the way that this debate has been framed since the terrible events of September 11th has been a national identification card or some sort of national ID system that would protect us from acts of terrorism. And based on the arguments I already made in my testimony, we can't build such a system on a set of faulty documents.

Many of those terrorists on September 11th had fake Social Security numbers. Actually all 19, according to the Inspector General last week, had such security numbers, some of them legally and some of them not. You can't establish motive or intent simply on the basis of knowing who someone is. It makes me nervous to think by having a traveler's ID or national ID card I could just pass through security unchecked without much more, and that to me doesn't create more security. In fact, it creates a false sense of security, too much dependence on technology.

If we are talking about State or Federal level efforts, we have to go back to the basic question, is this even an effective security measure to begin with?

Ms. SCHAKOWSKY. Anyone else burning to respond because I do have another question? Let me ask you this, is there a place for these incredible new technologies, biometrics, palm, all those things? I mean, should we be looking for ways to utilize them more effectively or do those lead into problem areas for us as well?

Anyone? Mr. Hoechst.

Mr. HOECHST. I would suggest there is a great many places for using them, but not necessarily should we have an expectation that tomorrow, we could use them to uniquely identify anyone who is on our soil, American or visiting. And that partly comes in limitations of the technology in its current state, but it partly comes just in the broad ability to adopt any such technology like that.

However, there are opportunities to use them where they are very effective. And this comes in, for example, authenticating yourself to secured areas. Perhaps we'd say you need to identify that you have certified—you need to identify biometrically that you are allowed to enter secured areas in an airport or whatever. And for that sort of smaller focus identification, we know there are a subset of people that are allowed to do this and we are going to confirm that you are one of that subset. They work quite well. For the general case of just saying, “Hey, I got a person here, let me look through all people to determine whether this person is this person,” they are still immature in that phase, I think.

Mr. SHNEIDERMAN. I want to confirm that on the technology side. These are promising technologies, but do not offer short-term hope for wide-scale dissemination. We've heard in the past voice recognition patterns and other technologies that might have been used, and these techniques are potentially interesting and they should be expanded and should be researched, but they are in the longer-term and should not be seen as a techno-fix in the short-term.

Ms. CORRIGAN. Although we are not the technology experts that you've got at the end of the table, I think our mantra is not all biometrics are created equal and not all uses of biometrics are created equal. We supply the same tests to those measures that we would to a national identification card. In the security context, the ACLU came out in support of the use of strengthened identification cards for air employees that need access to secure areas, including the use of biometrics on those cards. The reason is that in those instances it's a limited and targeted use of the biometric, and also you're able to take the thumbprint or you're able to take the iris scan under very controlled conditions, which makes a difference in the effectiveness and error rates of biometric technology.

Mr. GOODMAN. May I venture a comment? I'm not sure at the moment whether we realize the extent to which certain technologies are already in play. And in an attempt to achieve security, I would like to give you a couple of quick examples in this regard. As you may know, there is something called CAPS, which is an acronym for Computer Assisted Passenger Screening. This is a system under which information is obtained in the reservation process to screen out passengers who may require additional security checks. The airlines are fairly widespread in their use of such a system.

Also manifests are at this time provided by airlines. A manifest is a list of the passengers on a flight which will be landing in due course at a given airport, and in that airport they receive an advanced copy of the list of the passengers on board to try to determine whether there is a possibility of either customs violations or immigration violations and the like. So already Big Brother, if you please, is watching very closely in certain instances to try to determine what's going on. In my judgment, these are both fully justified in the present circumstances of tension. And I would again repeat, in the context of a war situation, anything we can do to utilize current technology to assist us in making identification of high-risk individuals is helpful. Normally you would not wish to do that. And you'd say in a civil libertarian sense, "Que sera sera," let it be and don't mess with this sort of thing. But I think it would be a great mistake when we know that we will probably be once again subject to a potential attack to allow ourselves to be in a solemn state to matters of this sort.

Mr. TURLEY. Could I add something? Obviously, I suggested a commission because I think this deserves more study. And I think that it's not just a technological issue that needs more study, but we need to look at the efficiency and viability of the systems. And if you have a single unified card it has to be integrated very often with at least some level of data base that creates its own issues. But putting that aside, I just wanted to disagree with Senator Goodman in one sense. I happen to think we do need more security.

But we have a long history of the government in times of crisis doing things that can only be described as moronic. And some of them are more than moronic, such as the internment of American citizens of Japanese origin. To simply say we are living in danger is not a justification for going boldly into these areas in the search for even a modicum increase in security. I think we have learned too much in terms of our history.

So I agree with Senator Goodman. I know that he intends this in the best sense. But I don't agree that should be the reason or the time schedule for us to act. I don't even believe this is necessarily going to add security. I mean these hijackers on September 11th had wallets that were bursting with false IDs. Adding another one is not going to reassure me. I would rather be reassured for my sons that when they inherit this country and this system that it's going to be given to them in the same condition that it was given to me. And that's my greatest concern, because frankly the Taliban is today's flavor of threat, and tomorrow there's going to be another group of fanatics. But I am more concerned in how we respond to the threat than the threat itself at the moment.

Mr. GOODMAN. May I remind us that had we taken a view that peoples' activities in the country are their own business unless they do something overtly wrong, that this possibly was what underlay the fact that we failed to realize that people are taking flying lessons, learning how to fly planes in midair, but neither to land them nor permit them to take off. And had we simply accumulated a little degree of intelligence data that indicated there were certain foreign nationals indulging in that type of flying lesson, it might have created a pattern of concern that would have possibly detected the advance notion of people plowing airplanes in tall buildings in our society.

I use that as an example because it does seem to me that there was an earlier reference to an intelligence breakdown. The use of vigilant intelligence and the need for both the horizontal and vertical communication of intelligence agencies in the United States is an absolute imperative at this time, and it is rather regrettable that we have been informed that the FBI and CIA have not adequately communicated with one another and certainly not adequately communicated with local law enforcement to permit vigilance at a time when it could be.

We want to practice preventive medicine. I don't want to wait until the next thing happens and say it's a pity it happened. Let's do something about it now. I would like to prevent it from occurring ever again, because anyone that lives in New York will be forever scarred by what's just happened, and that is why I am taking an intense view of these discussions at this moment.

Ms. SCHAKOWSKY. Thank you to all of you. I want to comment on this important discussion that we have been having. I think the example of flying lessons conducted by a company that gave them—what turned out to be a terrorist is an example of ways in which our current infrastructure failed us and the ability to communicate information brokedown, and we certainly are all interested in making sure that we fill in the cracks and make a seamless flow of information to the extent that we can. But I have to say, Senator Goodman, that I, too, feel that particularly at this time when we're all in a state of reflection about what is most precious about the United States, what are the things that make us unique and are so worth protecting, that we must proceed very cautiously, perhaps even more cautiously than when things are just clicking along so smoothly, so that we don't make the kinds of overreaching mistakes that we did when we interned the Japanese. And I know that you are certainly not talking about that kind of activity, but I think it is somewhat of a slippery-slope in that we have to be very careful that we don't install permanent—one reason, for example, that I voted no on a bill that I thought had many good provisions, the bill, which I felt shouldn't have been called the Patriot Act, because I believe myself to be a patriot, but I voted no on that. So I think we have to be very, very careful as we proceed forward. And I think that this conversation today and all of the witnesses, both panels, contributed to the kind of thoughtful debate that we need to have, and I appreciate it very, very much.

Mr. HORN. Well, I wanted particularly to appreciate what the ranking member did about the terrible breach of the Constitution with the Japanese Americans going into internments. I am proud to say my mother, who was director of welfare in her county, she opened up and said that is just wrong. And the only person I know of who was elected who was against that was Roosevelt and General DeWitt—just went ahead of everything, putting people in internment camps, even going with the Army to Peru, and so forth. But the only elected person was a very interesting gentleman named Harry Kane, the mayor of Tacoma, where many Japanese Americans were, and he later was a U.S. Senator and then President Eisenhower made him head of the Subversive, whatever board it was in those days, and he had the guts to stand it. And I had lunch with the Chief Justice Earl Warren just before he died, about 3 months before, and that was, he felt, the biggest mistake. And he was a wonderful man and very strong on civil liberties and—but one gets swept up in that and they do it. But it's wrong, and we don't want to see that happen again.

So let me just ask one or two questions and we'll close it out. Mr. Hoechst, Mr. Ellison has offered to provide the data bases for free for Oracle. Does this include maintenance, technical support and upgrades? As long as you are in a Santa Claus mood, I just thought I'd——

Mr. HOECHST. I would not venture to be able to speak for him on what's intended there. I would like to describe the nature of the intent of that offer, which was to take advantage of the resources and the enthusiasm that commercial organizations like Oracle and others have to facilitate action. So Larry's comments, I believe, were to try and remove any roadblocks required to facilitate action toward building systems that can share information. And if what we can do is provide free software or free maintenance on software or free services that can help us in a tactical way to stimulate action rather than be roadblocks that cause processes to languish, then we will do that.

Mr. HORN. I have one question for Ms. Corrigan. How would a consolidated identity system invade the privacy of individuals any more than the current systems, Social Security, driver's licenses, passports and—we have that now.

Ms. CORRIGAN. Actually, we also have something called the Privacy Act, which is rooted in one basic principle, and that is information collected for one purpose. So whether it's by the Museum of Modern Art in New York or whether it's by the Social Security Administration, information collected for that purpose shouldn't be used for another purpose unless subject to one of the exceptions outlined in the law. And we at the ACLU are very concerned about the misuse of Social Security numbers and privacy violations that go on everyday. But one of the biggest protections of privacy is actually the decentralized nature of the data. It is one thing for my doctor to have access to my personal health information. It's another thing for law enforcement to have my arrest record. But it's a completely different thing for people to combine those pieces of information and come up and marry them so you can come up with a whole profile of my life. And as I mentioned before, one accident, you know, in the Federal Government unfortunately has been subject to either accidents in terms of security on the Web or unfortunately employees who are corrupt and sell or use and misuse that information, that, again, there's a difference when you have separate data bases versus the marrying of the information.

Mr. HORN. I'll tell you, every hearing we have had on privacy, and that is we wanted to make sure and the Speaker mentioned it this morning, you make a felony out of it. We had one of our colleagues when I came into the Congress, her medical file had been put in the papers. And why? A disgruntled employee or whatever. And that's why people have to be very careful of any files in a doctor's office in particular.

Mr. SHNEIDERMAN. I would like to speak to that issue. There's a long history of attention between centralized and decentralized systems and there are two issues. One is as Ms. Corrigan described. The centralized facilities allow a single point of attack, single point of destruction, a single point of violation and therefore the magnitude of the violation is greater. The capacity of the computer to amplify power to do good also amplifies the power to do evil. And therefore someone can search across a much larger data set in that way.

But the other interesting point about the multiple or diversified, decentralized approach, actually it stimulates creative designs by having independent explorations and involves much more effective best practices if they are then shared and copied by the others, which is again why I encourage the collaboration by the way of the National association of State CIOs so that the best practices of each of the 50 States can then be repeated and disseminated widely. And that's truly one of the strengths of the decentralized approach.

Mr. HORN. I am going to thank the staff now and then have a closing bit of where I think this is going. And the person on my left is J. Russell George, the staff director and chief counsel for the subcommittee. And Bonnie Heald in the back is the deputy staff director. Darin Chidsey is a professional staff member. Mark Johnson, clerk. Earl Pierce, professional staff member. Jim Holms, intern. And then for the ranking member here, David McMillen, professional staff member. And Jean Gosa, minority clerk. Our court reporters, Lori Chetakian and Nancy O'Rourke, and we thank you.

The hearing was not intended to resolve the national identification issue, but merely to advance the debate in light of the September 11th attacks and the changed world in which we now live. Our witnesses provided a variety of perspectives and brought a great deal of expertise to the discussion. We are only beginning to explore this complicated issue. But one thing is certain, the September 11th attacks, as horrifying as they were, have brought out the best in America.

One small but important example of the Nation's strength is the ability to conduct this calm, civil but vigorous discussion of whether America needs a national identification system and, if so, how to go about creating it. Ultimately we can trust the American people and their representatives to make the right decision.

And with that, we are adjourned.

[Whereupon, at 1:50 p.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

"Does America Need a National Identification Card?"

United States House of Representatives'

Committee on Government Reform
Subcommittee on Government Efficiency, Financial
Management, and Intergovernmental Relations

November 16, 2001

Presented by:

The National Licensed Beverage Association
20 South Quaker Lane
Suite 230
Alexandria, VA 22314

For additional information please contact David Germroth
NLBA government affairs representative at 703-660-9245

On behalf of the 12,000+ small business members of the National Licensed Beverage Association, we greatly appreciate the opportunity to present the retail licensed beverage industry's views on the problems associated with the current identification system in the United States. In addition, we would like to address why the federal government should not mandate the use of a national identification card as a primary form of identification.

There has been considerable discussion from Congress, as well as support from the public since the September 11, 2001 attacks, to mandate the use of a national identification card. This proposed card would be the primary identification for almost all transactions, including opening a bank account, cashing a check, and buying a plane ticket. Those who support a national identification card refer to all of the problems with false identification and reference a recent poll that indicated a majority of Americans support a national identification card.

A national identification card would be used as a "national identifier," similar to a social security number. However, as evidence has shown, a social security number is a tool often used to create false identification cards.

Recently, Social Security Administration officials and others questioned whether procedures used in issuing Social Security numbers and retiring them after a person's death are adequate, in light of the uses to which the numbers are applied as a "national identifier" in social programs and financial markets. While concerns about using falsified documents to obtain Social Security numbers and identity theft have been raised in conjunction with financial fraud, this subject is of heightened urgency following reports that access to Social Security numbers facilitated the activities of the September 11 hijackers and one alleged accomplice.

As you already know, 13 of the 19 hijackers obtained Social Security numbers legally, offering visas and other documents, while the remaining six obtained them fraudulently. One alleged accomplice of the hijackers had been using the Social Security number of a New Jersey woman who died 10 years ago. It is believed that the balance of the hijackers would not have received Social Security numbers had government systems been properly integrated -- especially between the Social Security Administration and the Immigration and Naturalization Service -- and current technology fully utilized. With Social Security numbers so integrated into Americans' daily lives, the nation must face up to the ambiguity over whether it is a national identifier and how its integrity should be protected, because once obtained, it allows an individual the ability to insert themselves into society below the radar screen.

A problem that licensed beverage retailers have faced in the past, and have successfully lobbied Congress to enact legislation against, is the illegal sales of false identification on the Internet. Nearly flawless counterfeit identification is widely available on the Internet and has been used in crimes ranging from fraud to murder. Web sites offer fake documents for sale, from a Social Security card for $40 to a birth certificate for $79 to a driver's license from any state for $90. Several hundred dollars will buy a full set of identification, including a military ID and a college diploma.

Some sites offer to manufacture the bogus IDs, complete with photos, while others offer templates on CD-ROMs for downloading, essentially providing do-it-yourself fake ID kits. The sites guarantee that the documents will come with requisite bar codes, holograms, seals and magnetic strips.

"The Internet business in fake identification allows criminals to operate anonymously all over the world," said Bruce Townsend, special agent in charge of the U.S. Secret Service's financial crimes division. "Technological advances have changed the landscape of financial crime and other kinds of crime as well," he said.

American teens anxious to flash drinking-age IDs, kidnappers in Tokyo, and an accused killer from New Jersey are among the many thousands who have used the documents, according to law enforcement officials.

In April, Gregory Marcinski, 23, of Brick, New Jersey, allegedly used a bogus computer-generated FBI identification in the course of killing his ex-girlfriend's new boyfriend. Authorities say Marcinski persuaded a Kentucky motel owner to let him search the victim's room. Once inside, Marcinski kidnapped, then strangled the man and later burned and buried his body in a New Jersey swamp, police said.

"You can become anyone you want -- an FBI agent, an Army sergeant, or take over the identity of someone you know, or even someone you don't," said Kirk Walder, an investigator for the U.S. Senate permanent subcommittee on investigations, which conducted a five-month probe of the phenomenon. "It's child's play."

Bogus Internet ID hustlers accounted for more than $100 million in fraudulent credit card bills last year, with the average take per bill running at about $20,000. The con men use the documents to develop new personas, open bank accounts, get credit cards, run up huge bills, and then default on payment.

Benito Castro of Boca Raton, Florida, assumed the identity of Dr. Charles Glueck, a Metairie, Louisiana dentist, for more than six months last year. Castro allegedly took advantage of Glueck's good credit, opened up more than 12 credit card accounts in the dentist's name, and ran up thousands of dollars in bills at a new address.

In a variation on this theme, Mark Diaz, a computer systems analyst from North Miami is charged with using false ID to obtain a $265,000 mortgage in a New Yorker's name last spring. Diaz allegedly searched the Internet to get information on Norman Brodeur of New York City and Boca Raton. With a fake driver's license and birth certificate in Brodeur's name, Diaz got the mortgage and deposited the check in a Florida bank. He was caught only after he applied for further loans in Brodeur's name.

Walder said Internet grifters often use pieces of fake ID to develop a cache of produced identification under an assumed name. "All you need for a passport is a driver's license and a birth certificate," said Walder.

Furthermore, the U.S. Passport Office seldom checks the ID presented if it looks authentic. "We issue 7 million new passports a year, and with that volume, we seldom take the extra step of checking to verify an address or the rest of an identity unless we had a special reason to believe you were not who you said you are, or we knew your license and birth certificate were fraudulent," said a State Department official, who asked that his name be withheld. "A good fake passport costs $10,000 on the street, if you know where to get one, but with the Net, you can save the $10,000, get the fake ID, and get a real passport under a false name."

Law enforcement officials said some of the entrepreneurs set up sites through Internet providers in foreign countries or otherwise disguise the origins of their sites.

"They're very difficult to track down," said James Hesse, chief intelligence officer of the Immigration and Naturalization Service's forensic documents lab. Although many laws can be used to prosecute those who use false identification to commit fraud, up until last year there was no federal statute that can be used against the Web site dealers because of the way they set up their sales.

William Sherman, a *Daily News* staff writer, wrote how his identity change began with a simple Internet surfer's query, "How can I obtain fake ID?" Sherman's challenge was to use the Internet to create a new identity for himself, build a portfolio of documentation acceptable to banks, credit card companies and a variety of government agencies including the U.S. passport office.

When he was done, after $300 worth of purchases at office supply and art stores and the help of a *Daily News* computer graphics specialist, he was a new man. William Sherman of New York City had become Sam Nathanson of Madison, N.J., with a laminated driver's license complete with photo and a birth certificate to prove it. He could disappear as Sherman and reappear as Nathanson and start a new life, legitimate, or illegitimate.

Sherman found a site offering free templates, or models, for IDs that could be downloaded and used by him to create the Nathanson documents. On the blank license, he put in the name Sam Nathanson with a nonexistent address and used accurate information on other vital statistics such as height, weight, eye color and age. Using a photo scanner, he downloaded his picture, appropriately sized, onto the template. With stencil paper bought at an art store, he created a model of the hologram and using the recommended expensive acrylics, painted it perfectly onto the document. Once laminated the fake identification was done -- Sam Nathanson, 270 Main St., Madison, N.J.

There are templates on the Internet for birth certificates as well, but Sherman took a shortcut and downloaded a real New Jersey certificate. Using the art program, he matched the typefaces and put in the new information on Sam Nathanson -- born Dec. 9, 1948, at 9:32 a.m., at Memorial Hospital of Burlington County, Mount Holly, N.J. At a midtown New York City branch of Citibank, Sherman asked to open an account, and produced the driver's license and a copy of a utility bill, along with the birth certificate.

A bank officer held the license to the light, turned it over, and showed it to a co-worker. Then she opened a book with color photographs of licenses from every state and checked his against the New Jersey sample. She looked from the license to the book and back again, checked the hologram against the light, and then handed the license back to him, satisfied that it was good.

A State Department official said the papers were good enough to get a passport. Sherman could have obtained credit cards, a legitimate New York driver's license, library cards, museum memberships, magazine subscriptions, a lease on a new apartment, moved to California, whatever. The possibilities were endless which is exactly what federal law enforcement officials said. Others have done that and more.

Stories like Sherman's and countless others who have used fake identification to illegally buy licensed beverages, or for perpetrating acts of evil, are why changes must be made to the current identification system in the United States. A national identification card, however, is not the answer.

Free Congress

For Immediate Release:
November 16, 2001

Contact: Steve Lilienthal 202.204.5304
slilienthal@freecongress.org

Statement of J. Bradley Jansen
Deputy Director, Center for Technology Policy of the Free Congress Foundation
National ID Shred In
November 16th, 2001

I'd like to thank Marc for putting this together and say that I am happy to applaud the leadership of other defenders of liberty and responsible government such as Reps. Ron Paul (R-TX) and Bob Barr (R-GA) who have prevented an effective national ID taking effect as a result of the immigration reform bill a few years ago. I am also encouraged by recent the comments of Supreme Court Justice Antonin Scalia who said that he would probably vote against it if there were a popular vote.

According to James Bamford, author of the only books on the National Security Agency, 9-11 was the greatest failure of intelligence in the history of this country. What is needed most in this country is for us to remedy the decline of professionalism and resulting scandals of our law enforcement and intelligence communities that we experienced under the Clinton years.

We should not be distracted from this fact when we hear excuses about a lack of tools or antiquated laws. It is far from clear that these National ID proposals will be effective preventing tragedies such as we experienced on September 11th. The closest thing we have to a national ID in this country now is our passport. However, it was reported that one of the highjackers of 9-11 used a stolen passport. The rightful owner notified authorities responsibly. Apparently, the State Department does not keep a list of passports that are reported stolen because this innocent man was named as a suspected terrorist.

Forgeries and other problems would also limit the usefulness to law enforcement.

A national ID would impose a huge unfunded mandate on the states that would have to pay for its compliance. Such a financial cost would only add insult to injury such a mandate would cause to our respect for federalism. Just look at the cost overruns of the "dead beat dads" database with all of its problems.

This misallocation of resources is not unusual where law enforcement follows an approach of mass surveillance of everyone all the time instead of focusing its resources to focus on the real threats to this country. We need to redirect those resources to hire agents to that know the languages, the cultures and try to infiltrate the identified groups that threaten us.

Turning to a national ID runs the risk that it will be used for unacceptable purposes. History is full of such examples such as religious prosecution: not just the Nazis and the Jews, but the military junta in Greece imposed religious identification that was not repealed for many years. Perhaps there are some who want to copy the success of the internal pass cards used under Aparteid. I'm sure others find the example of the Soviet Union a better example to follow.

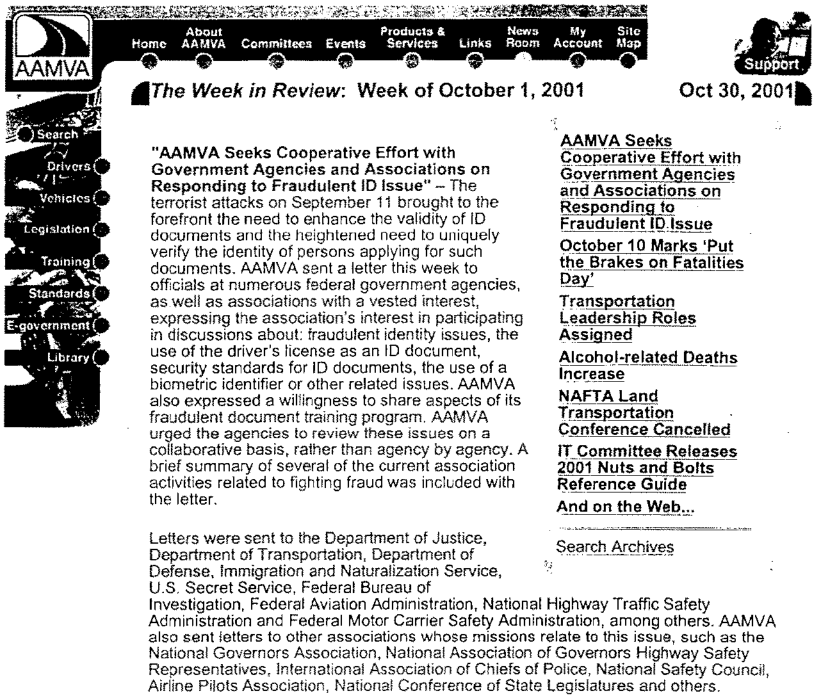
Most realistically, such a scheme would create problems with identity fraud and other misuses of data:

- Former Chicago Police Department Chief of Detectives William A. Hanhardt looked up the driver's license, car registration, and other information concerning jewelry salesmen on department computers and the NLETS system (a non-profit corporation organized by state law-enforcement agencies) to run an elaborate jewelry-theft ring;
- Former FDIC employee Theresa Hill used data for which she had access to commit identity fraud and charge tens of thousands of dollars to credit cards in other peoples' names;
- IRS employees look up information about celebrities;
- A Financial Crimes Enforcement Agency (FinCEN) employee used his access of banking and other personal records for independent research about his girlfriend's mother; and
- Michigan state Detective Sgt. Artis White earned the dubious distinction of being named the National Consumer Coalition Privacy Group's (www.nccprivacy.org) first Villain of the Week for allegedly stalking his estranged wife using Michigan's Law Enforcement Information Network (LEIN).

Our first priority should be to hold our nation's finest to the highest of standards of professionalism as our best way of having a safe and secure country. We should shred this national ID proposal and put in the trashcan of bad ideas where it belongs.

For more information about Free Congress Foundation:

http://www.freecongress.org



The Week in Review: Week of October 1, 2001

Oct 30, 2001

"AAMVA Seeks Cooperative Effort with Government Agencies and Associations on Responding to Fraudulent ID Issue" – The terrorist attacks on September 11 brought to the forefront the need to enhance the validity of ID documents and the heightened need to uniquely verify the identity of persons applying for such documents. AAMVA sent a letter this week to officials at numerous federal government agencies, as well as associations with a vested interest, expressing the association's interest in participating in discussions about: fraudulent identity issues, the use of the driver's license as an ID document, security standards for ID documents, the use of a biometric identifier or other related issues. AAMVA also expressed a willingness to share aspects of its fraudulent document training program. AAMVA urged the agencies to review these issues on a collaborative basis, rather than agency by agency. A brief summary of several of the current association activities related to fighting fraud was included with the letter.

Letters were sent to the Department of Justice, Department of Transportation, Department of Defense, Immigration and Naturalization Service, U.S. Secret Service, Federal Bureau of Investigation, Federal Aviation Administration, National Highway Traffic Safety Administration and Federal Motor Carrier Safety Administration, among others. AAMVA also sent letters to other associations whose missions relate to this issue, such as the National Governors Association, National Association of Governors Highway Safety Representatives, International Association of Chiefs of Police, National Safety Council, Airline Pilots Association, National Conference of State Legislatures and others.

AAMVA Seeks Cooperative Effort with Government Agencies and Associations on Responding to Fraudulent ID Issue

October 10 Marks 'Put the Brakes on Fatalities Day'

Transportation Leadership Roles Assigned

Alcohol-related Deaths Increase

NAFTA Land Transportation Conference Cancelled

IT Committee Releases 2001 Nuts and Bolts Reference Guide

And on the Web...

Search Archives

AAMVA Projects Dealing with the Driver License Document and Its Issuing and Support System

1. Driver License/ID Document Standard

AAMVA is involved in creating a driver license document standard, both nationally and internationally. National and international standards insure that documents are interoperable among the issuing jurisdictions—the bar code on an Iowa license may be read by a trooper in New York and vice versa. On a national level, AAMVA has developed and published the AAMVA Driver License/ID Card Standard that is being used by most states for creating a driver license and ID card. AAMVA is in the process of further improving this standard and working with more states to ensure that they adhere to its provisions when they create a new document. We continue to work towards further harmonization among the states in using the standard. Internationally, we are developing a standard for an international drivers license that will enable a more secure alternative to the current "International Driver Permit" that could serve the dual purpose of a domestic drivers license and be recognized internationally. Both the national and international driver license standards have provisions for machine-readable technologies (bar codes, magnetic stripes, and smart cards) and biometrics.

2. Uniform Identification Practices Model Program

AAMVA developed a model administrative procedures program for issuance of driver licenses and ID cards that is used by most states. AAMVA is currently revising this model program. Major topics of the model program are issuance procedures (initial, renewal and duplicates), unique identifiers, communication with Social Security and INS, name changes, maintenance of an identification document list, residency and legal presence, foreign documents, sanctions, security features, and technology. We continue to work toward further harmonization among the states by encouraging them to use the model program.

3. Fraud Prevention Programs

For years AAMVA has provided Fraudulent Document Recognition Train-the-Trainer courses for state and provincial motor vehicle agencies. We are updating this course in cooperation with Lt. David Myers of the Florida Alcoholic Beverages and Tobacco Division and the Forensic Services Division of the United States Secret Service. Our aim is to involve other federal agencies in this process. We are also addressing other issues (e.g., ID theft, internal fraud) and support our membership in dealing with them. We are creating a "best practices" document that will provide an overview of how state and provincial motor vehicle and law enforcement agencies deal with these issues.

4. Networks / Databases (Movement of Information)

AAMVAnet, a subsidiary of AAMVA, manages and operates the Commercial Driver License Information System, which is designed as a clearinghouse for commercial drivers. AAMVAnet is also involved with the National Driver Register/Problem Driver Pointer System owned by the National Highway Traffic Safety Administration. AAMVAnet has cooperated in a study for Congress evaluating driver licensing information programs and assessing technologies. AAMVAnet is working with federal agencies in looking at incorporating different driver licensing information systems into one system (DRIVerS).

AAMVA is also designated by the Department of Justice to operate the new National Motor Vehicle Title Information System. This system allows jurisdictions to instantaneously verify the validity of titles prior to issuing new titles. This inhibits title fraud and auto theft by making it harder to title stolen vehicles.

5. Foreign Reciprocity

AAMVA recently finalized a foreign reciprocity resource guide for its membership. Major topics discussed in the guide are:

- Legal Considerations
- Model and Existing Driver's License Reciprocity Agreements
- Issues to Consider before entering into a Reciprocity Agreement
- Model and Existing Enabling Legislation
- Driver Licensing Standards
- Foreign Driver License Assessment and Verification of Driver Status

AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATORS EFFORTS NEEDED TO IMPOVE SAFETY AND SECURITY

CURRENT CONDITION

- A unique system exists in all 51 U.S. jurisdictions supporting the issuance of driver licenses and identification cards. This system lacks uniformity, but still provides for reciprocity.

- All 51 U.S. jurisdictions use security features on their driver licenses and identification cards, but no standardized security features are used uniformly nationwide. This poses a difficult challenge for law enfcrcement and verification.

- The driver's license is the recognized form of identification across the U.S. and is used as the source credential for many other transactions including the issuance of a U.S. passport.

- AAMVA currently electronically links with all U.S. jurisdictions through a secure, private network and a reliable and scalable infrastructure exists.

- Source documents used to obtain a driver's license or identification card have varying degrees of security and many can be easily altered.

- Limited Federal oversight is exercised on the issuance of drivers' licenses and identification cards and limited federal requirements are mandated. The Commercial Drivers License Program is an exception.

- While some states rigorously audit the process and procedures used to issue valid drivers licenses and identification cards, no standardized federal requirements exist for compliance.

- Penalties for the fraudulent issuance of drivers licenses and identification cards are minimal and are for the most part misdemeanors and in some cases summary offenses.

- The determination and verification of legal presence and residency varies greatly from state to state.

AAMVA'S ACTIONS AND RECOMMENDATION

- AAMVA has taken a leadership role in representing its members (the 51 U.S. jurisdictions and 13 Canadian provinces) in advancing improvements to the licensing and validation process to ensure identification security.

AAMVA'S ACTIONS AND RECOMMENDATION

- Its Board of Directors has established a Special Task Force on Identification Security. The Task Force is currently working on four key areas: technology, new issuance, residency and document security.

- A stronger Federal and State Partnership is needed to strengthen the licensing and identification process in all jurisdictions and to ensure uniformity and consistency.

- A system, similar to the current Commercial Drivers License Information System (CDLIS), is necessary to ensure that only qualified individuals are licensed and issued identification cards. This system must interconnect to all jurisdictions and with other key databases such as Social Security Administration, Vital Statistics and Immigration and Naturalization Services. This system would help ensure security and safety with one license for one person and one identification card for one person only in one jurisdiction at a time.

- The current AAMVA network and information system should be used as the conduit for any new system connecting the jurisdictions.

- Federal funding is necessary to ensure that all jurisdictions are able to comply with uniformity and standardization requirements.

NATIONAL AND CONGRESSIONAL LEADERSHIP NEEDED

- Leadership is needed to help AAMVA and all U.S. jurisdictions improve the issuance of drivers' licenses and identification cards so that these products can be recognized nationwide as a reliable form of identification.

- AAMVA's Special Task Force on Identification Security will complete its recommendations and improvement strategies in January. These strategies should serve as a blueprint for congressional action.

- AAMVA must continue to be the recognized leader in the coordination of this effort and should be recognized as the standards authority.

- National legislation is necessary to ensure safety, identification security and improvements to the identification verification process.

- DRIVerS, an information system, recommended by Congress in the TEA-21 Transportation Authorization, must move forward and be funded and implemented in all U.S. jurisdictions.

AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATORS (AAMVA) EXECUTIVE COMMITTEE RESOLUTION

WHEREAS, AAMVA is an international organization and recognized as the authority on matters relating to the issuance of driver's licenses and other secure identification documents, and

WHEREAS, AAMVA is in a unique position with its jurisdictional members, law enforcement community, industry partners and relationships with other key communities to be a driving force for change and improvement in the issuance of secure driver's licenses and identification credentials, and

WHEREAS, AAMVA's members have the experience, knowledge and infrastructure necessary to help ensure that driver's licenses and other identification credentials are issued with the utmost security and public confidence, and

WHEREAS, AAMVA has a secure, private computer network connected to all U.S. and Canadian jurisdictions to verify and exchange identification information, and

WHEREAS, AAMVA is the recognized leader in the development of uniform standards for U.S. and Canadian jurisdictions relating to the issuance of driver's licenses and identification credentials, and

WHEREAS, AAMVA recognizes that the driver's license and jurisdiction issued identification cards have become the "de facto" national identification card used by law enforcement, retailers, banks and other establishments requiring proof of identification, and

WHEREAS, AAMVA understands the importance and the urgency of continuing to improve the determination and reliability of identity in the issuance of driver's licenses and identification credentials for national security and safety purposes, be it

RESOLVED, That the AAMVA Chair of the Board hereby establishes a Special Task Force on Identification Security, and

RESOLVED FURTHER, That the Special Task Force on Identification Security be charged with developing an overall strategy on enhancing the issuance of secure identification credentials for driver licensing and photo identification purposes, and

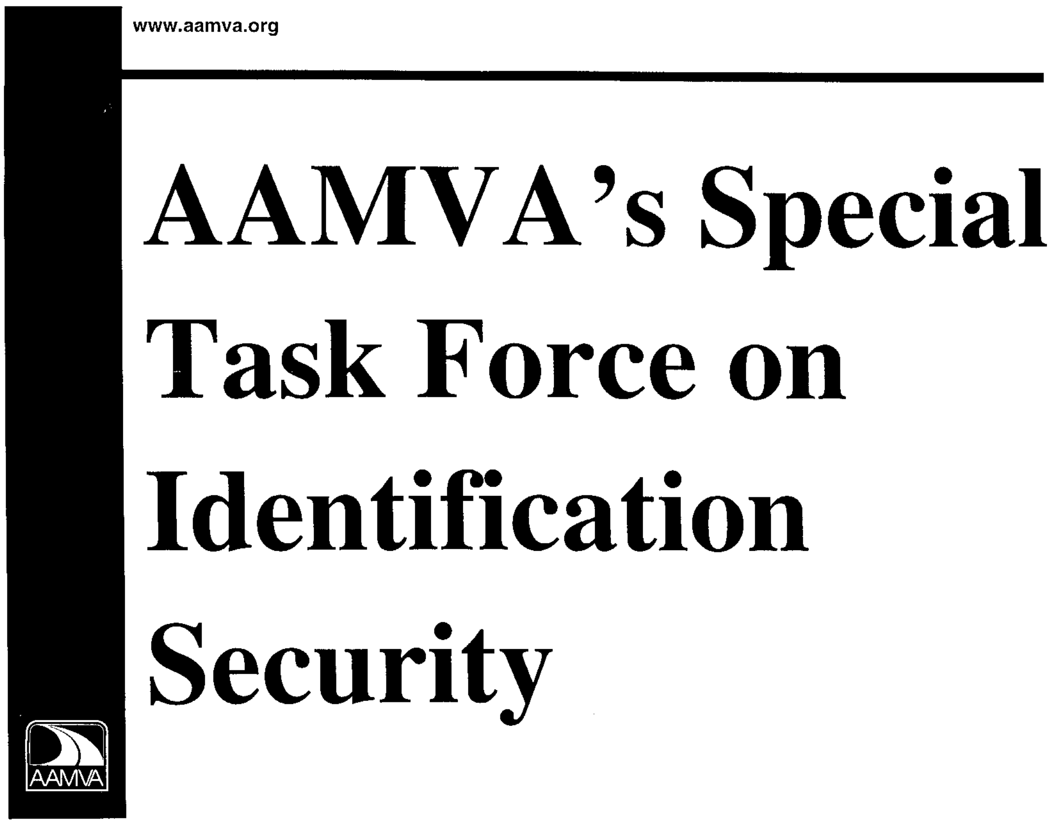
RESOLVED FURTHER, That the Special Task Force on Identification Security develop short- and long-term priorities and actions relating to improving the security of driver licensing and identification credentials, and

RESOLVED FURTHER, That the Special Task Force on Identification Security build relationships with other key stakeholders including industry, Congress and federal agencies, such as the U.S. Department of Transportation, the U.S. Department of Justice, the U.S. Department of State, the U.S. Immigration and Naturalization Services, the U.S. Social Security Administration and the President's Office of Homeland Security, to improve coordination and credentialing security, and

RESOLVED FURTHER, That the Special Task Force on Identification Security make a full report with its recommendations to the AAMVA Board of Directors at its Winter Board Meeting in January 2002.

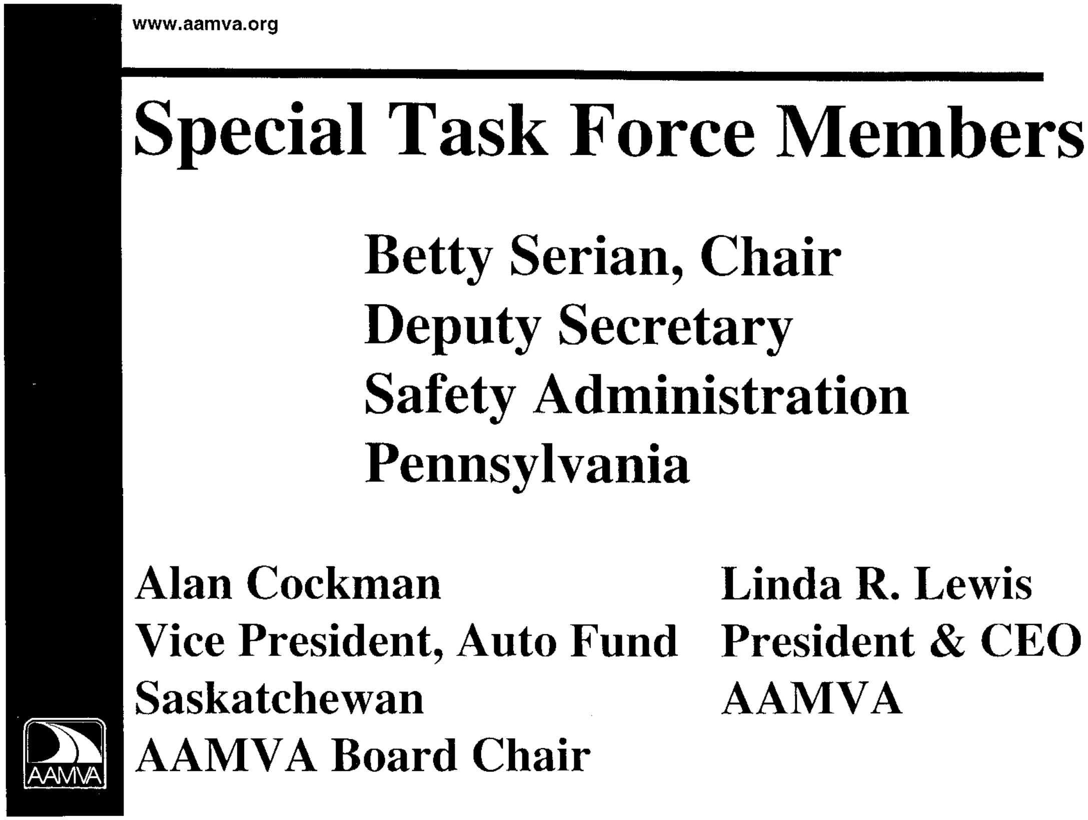
CREATED BY THE AAMVA EXECUTIVE COMMITTEE ON OCTOBER 24, 2001

Alan Cockman, Chair of the AAMVA Board of Directors
Betty Serian, First Vice Chair of the AAMVA Board of Directors
Keith Kiser, Second Vice Chair of the AAMVA Board of Directors
Jerry Dike, Secretary of the AAMVA Board of Directors
Martha Irwin, Immediate Past Chair of the AAMVA Board of Directors
Novella Crouch, Treasurer of the AAMVA Board of Directors
Linda Lewis, President and CEO of AAMVA



www.aamva.org

AAMVA's Special Task Force on Identification Security



www.aamva.org

Special Task Force Members

Betty Serian, Chair
Deputy Secretary
Safety Administration
Pennsylvania

Alan Cockman
Vice President, Auto Fund
Saskatchewan
AAMVA Board Chair

Linda R. Lewis
President & CEO
AAMVA

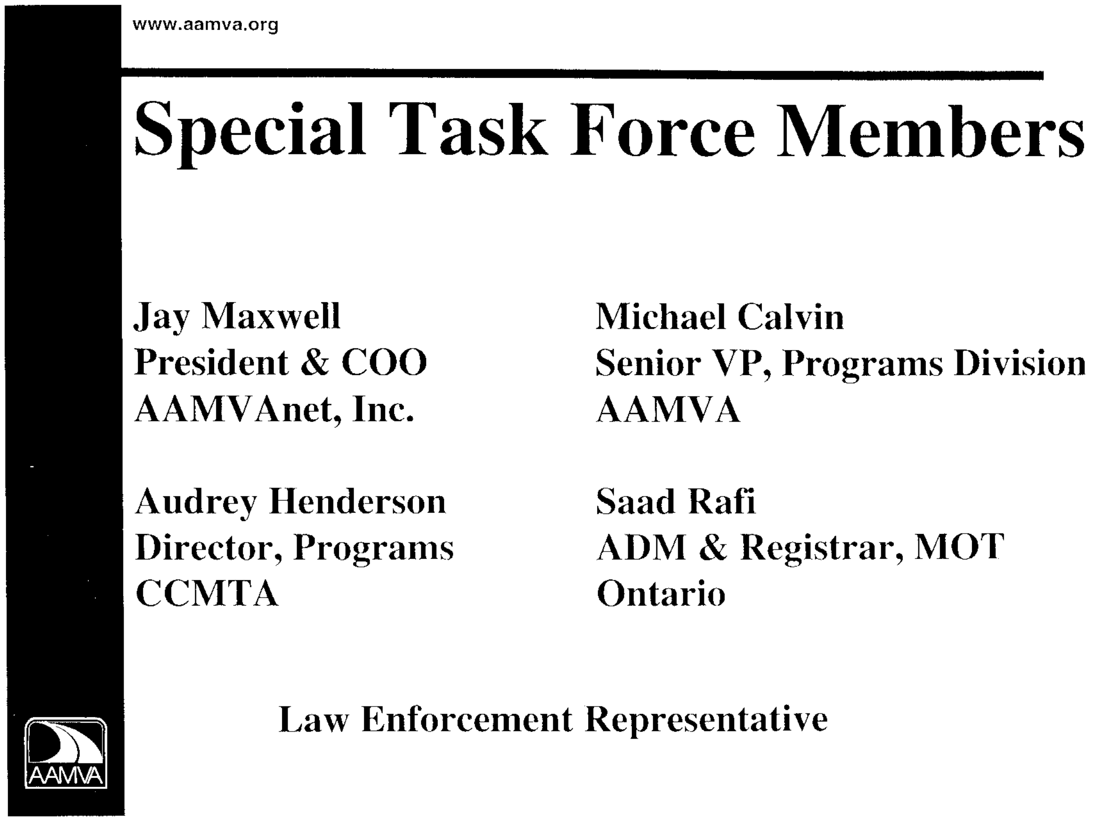
Special Task Force Members

W. Pat Scheffer
Director
Driver & Vehicle Services
New Jersey

Joseph Sanders
Director
Office of Document Prod.
New York

Jerry L. Dike
Director
Vehicle Titles / Reg. Div.
Texas

Michael Anderson
Assistant Chief
Administration
Texas



www.aamva.org

Special Task Force Members

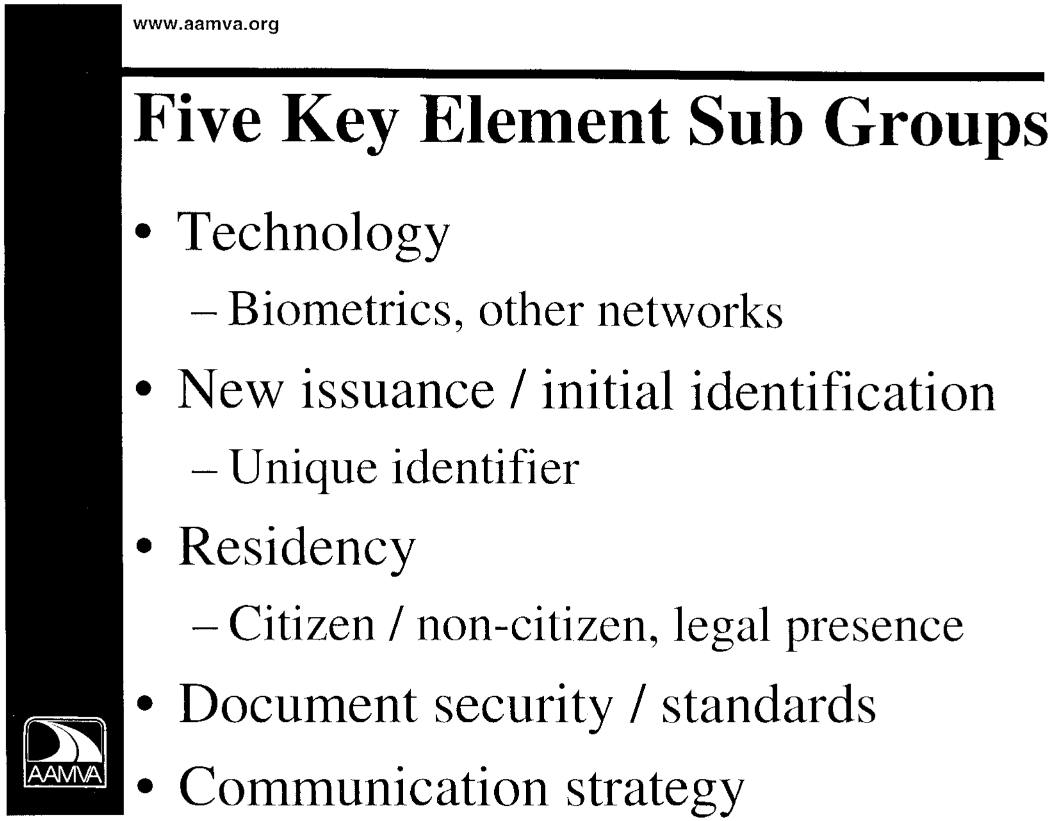
Jay Maxwell
President & COO
AAMVAnet, Inc.

Michael Calvin
Senior VP, Programs Division
AAMVA

Audrey Henderson
Director, Programs
CCMTA

Saad Rafi
ADM & Registrar, MOT
Ontario

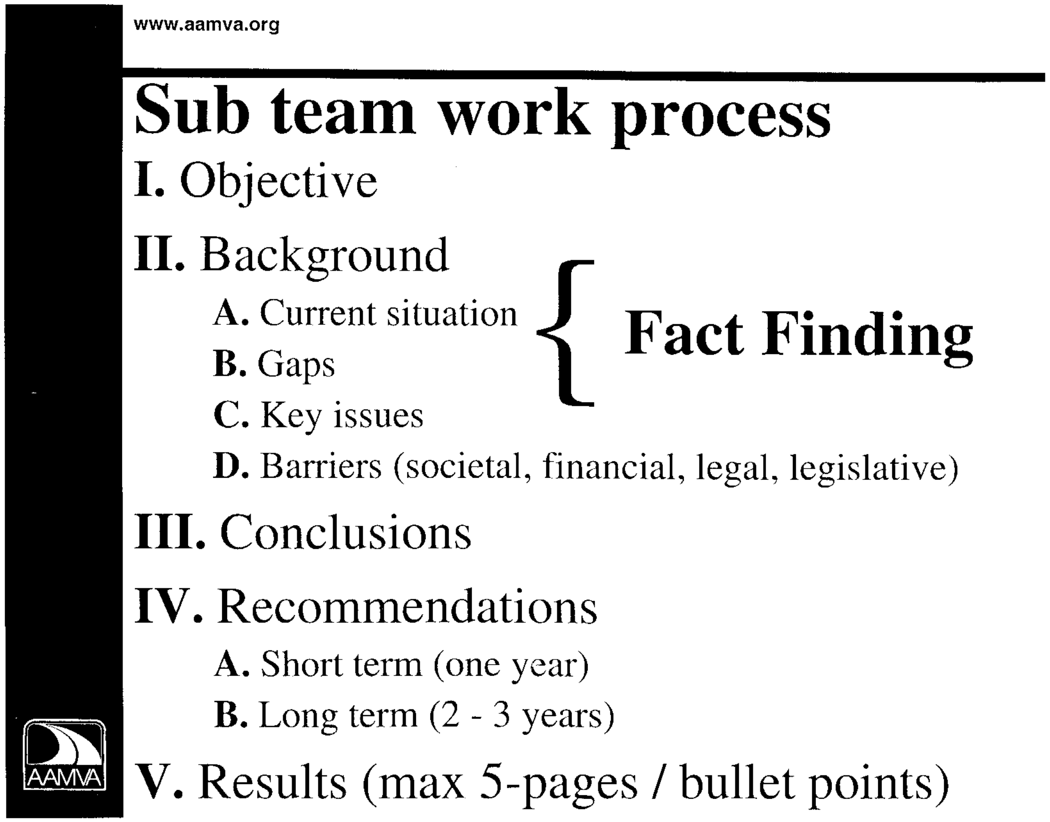
Law Enforcement Representative



www.aamva.org

Five Key Element Sub Groups

- Technology
  - Biometrics, other networks
- New issuance / initial identification
  - Unique identifier
- Residency
  - Citizen / non-citizen, legal presence
- Document security / standards
- Communication strategy



www.aamva.org

Sub team work process

I. Objective

II. Background

- **A.** Current situation
- **B.** Gaps
- **C.** Key issues
- **D.** Barriers (societal, financial, legal, legislative)

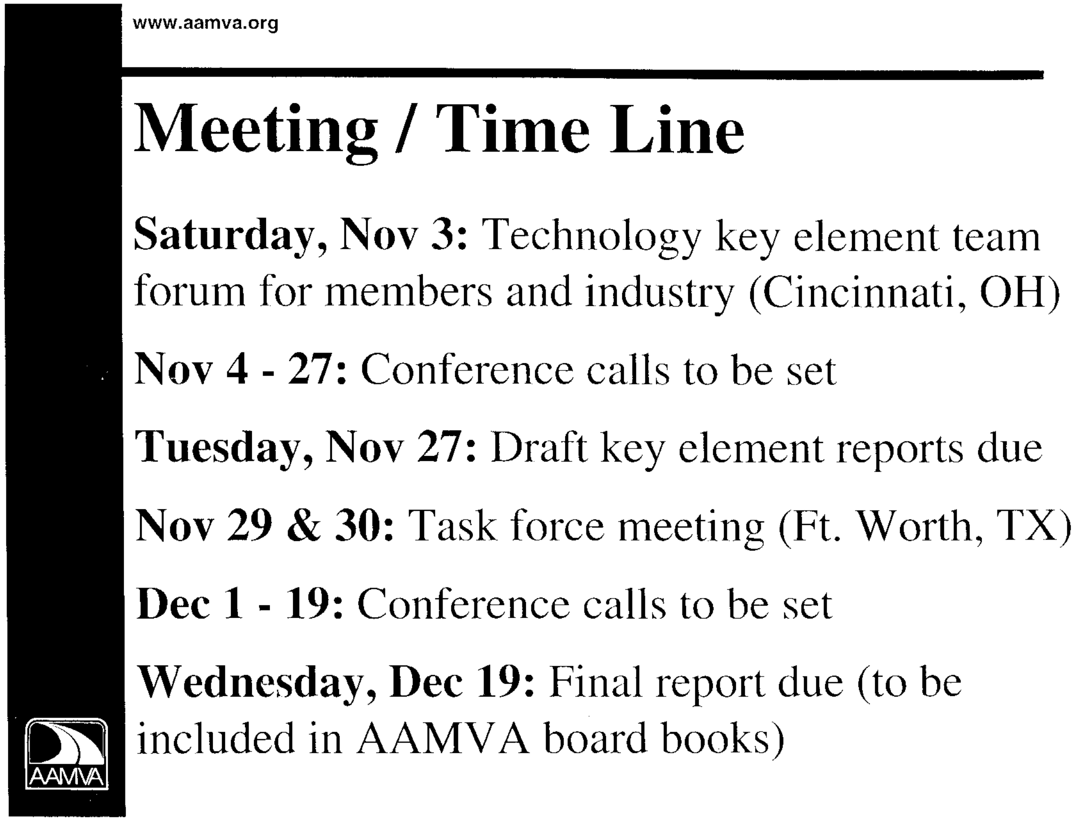
{ **Fact Finding**

III. Conclusions

IV. Recommendations

- **A.** Short term (one year)
- **B.** Long term (2 - 3 years)

V. Results (max 5-pages / bullet points)



www.aamva.org

Meeting / Time Line

Saturday, Nov 3: Technology key element team forum for members and industry (Cincinnati, OH)

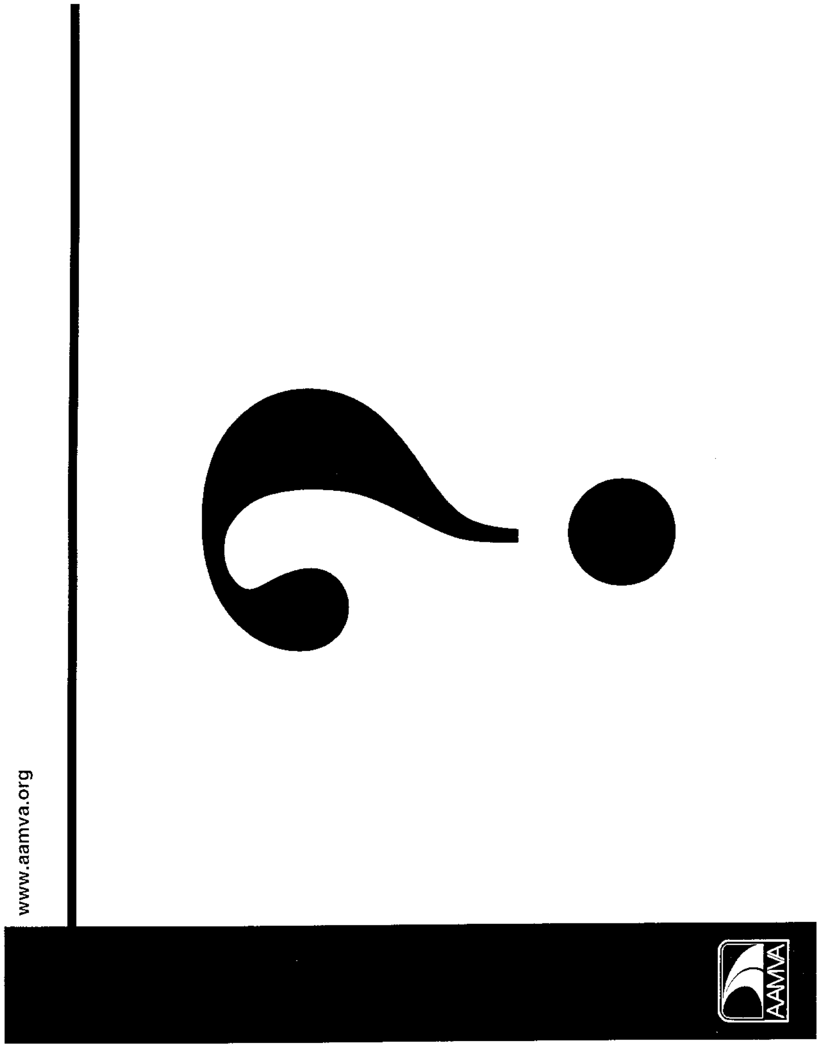
Nov 4 - 27: Conference calls to be set

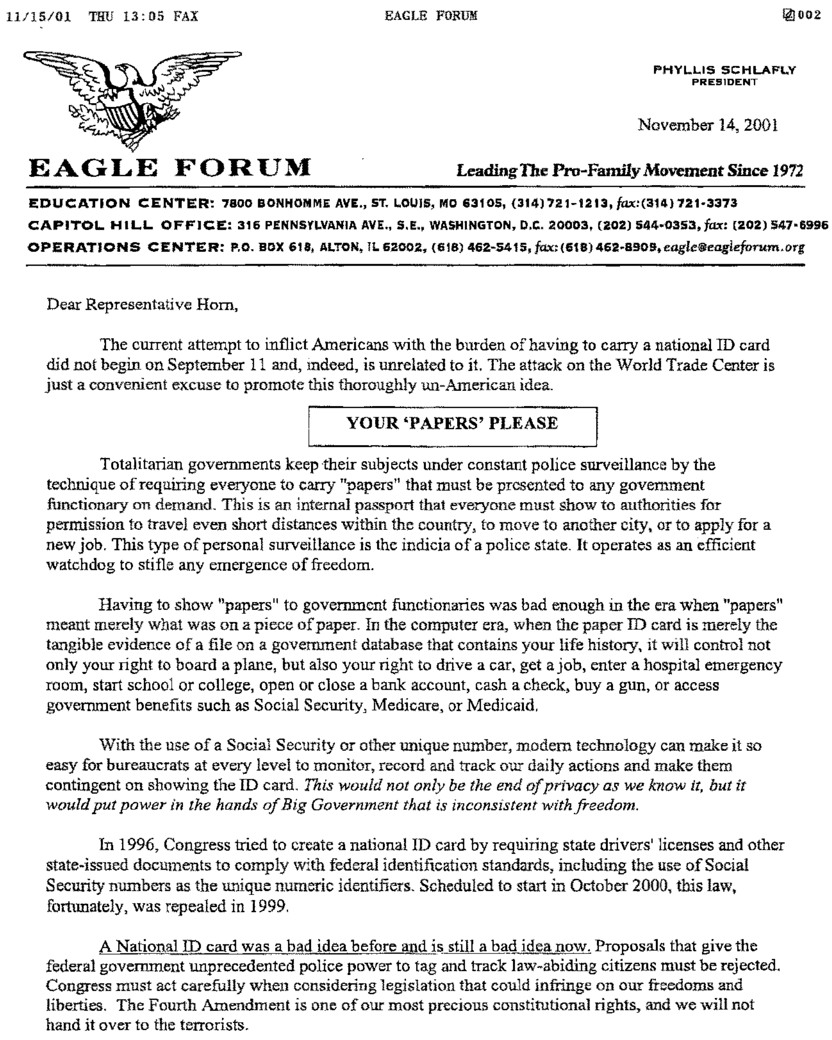
Tuesday, Nov 27: Draft key element reports due

Nov 29 & 30: Task force meeting (Ft. Worth, TX)

Dec 1 - 19: Conference calls to be set

Wednesday, Dec 19: Final report due (to be included in AAMVA board books)


www.aamva.org
AAMVA



11/15/01 THU 13:05 FAX EAGLE FORUM ☒002

PHYLLIS SCHLAFLY
PRESIDENT

November 14, 2001

EAGLE FORUM *Leading The Pro-Family Movement Since 1972*

EDUCATION CENTER: 7800 BONHOMME AVE., ST. LOUIS, MO 63105, (314) 721-1213, *fax:* (314) 721-3373
CAPITOL HILL OFFICE: 316 PENNSYLVANIA AVE., S.E., WASHINGTON, D.C. 20003, (202) 544-0353, *fax:* (202) 547-6996
OPERATIONS CENTER: P.O. BOX 618, ALTON, IL 62002, (618) 462-5415, *fax:* (618) 462-8909, *eagle@eagleforum.org*

Dear Representative Horn,

The current attempt to inflict Americans with the burden of having to carry a national ID card did not begin on September 11 and, indeed, is unrelated to it. The attack on the World Trade Center is just a convenient excuse to promote this thoroughly un-American idea.

YOUR 'PAPERS' PLEASE

Totalitarian governments keep their subjects under constant police surveillance by the technique of requiring everyone to carry "papers" that must be presented to any government functionary on demand. This is an internal passport that everyone must show to authorities for permission to travel even short distances within the country, to move to another city, or to apply for a new job. This type of personal surveillance is the indicia of a police state. It operates as an efficient watchdog to stifle any emergence of freedom.

Having to show "papers" to government functionaries was bad enough in the era when "papers" meant merely what was on a piece of paper. In the computer era, when the paper ID card is merely the tangible evidence of a file on a government database that contains your life history, it will control not only your right to board a plane, but also your right to drive a car, get a job, enter a hospital emergency room, start school or college, open or close a bank account, cash a check, buy a gun, or access government benefits such as Social Security, Medicare, or Medicaid.

With the use of a Social Security or other unique number, modern technology can make it so easy for bureaucrats at every level to monitor, record and track our daily actions and make them contingent on showing the ID card. *This would not only be the end of privacy as we know it, but it would put power in the hands of Big Government that is inconsistent with freedom.*

In 1996, Congress tried to create a national ID card by requiring state drivers' licenses and other state-issued documents to comply with federal identification standards, including the use of Social Security numbers as the unique numeric identifiers. Scheduled to start in October 2000, this law, fortunately, was repealed in 1999.

A National ID card was a bad idea before and is still a bad idea now. Proposals that give the federal government unprecedented police power to tag and track law-abiding citizens must be rejected. Congress must act carefully when considering legislation that could infringe on our freedoms and liberties. The Fourth Amendment is one of our most precious constitutional rights, and we will not hand it over to the terrorists.

THE REAL PROBLEM: IMMIGRATION

Americans and Members of Congress must understand that the 9-11 hijackings are a problem of the U.S. government allowing illegal aliens to roam freely in our country, and promiscuously issuing visas without proper certifications. It's also a problem of the government failing to enforce current immigration and visa laws, and failing to deport illegal aliens including those who overstay their visas. At least 16 of the 19 hijackers fit in one or more of these categories.

For more than two weeks prior to 9-11, the FBI had been trying to find one of the hijackers whom the CIA had spotted meeting with a suspect in the bombing of the USS Cole. But all the FBI had to go on was his visa application, which listed his address as "Marriott, New York City" (where there are ten Marriott hotels and he never went to any of them).

The U.S. State Department is a big part of the problem. Some 3,700 consular officers worldwide approve 80 percent of the 8 million visa applications every year. Checking the background of every alien applicant is an impossible task at the current application level.

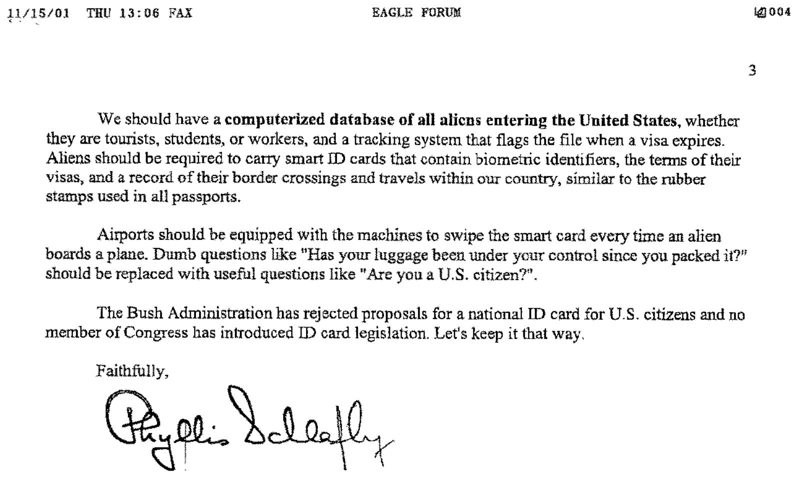
Security starts at our borders. The United States has been granting 250,000 visas a year to Middle Easterners, including aliens from Iraq, Libya, Algeria, Syria, Egypt, and Afghanistan. Applicants from Saudi Arabia can get "Multiple Use" two-year visas, and beginning June 25, can take advantage of an express visa service that waives the requirement of personal appearance. 60,000 visas are issued to Saudi Arabians; was every one of them thoroughly reviewed? Since the State Department clearly cannot handle the application level, the number of Middle Eastern visas should be cut from 250,000 to 2,500 until the technology is in place to screen out and track dangerous aliens. Furthermore, *no visas of any kind should be issued to countries that fail to repudiate terrorists.*

The Immigration Reform and Immigrant Responsibility Act of 1996 requires aliens crossing the Mexican border to present biometric, machine-readable border crossing cards. This law went into effect on October 1, 2001, but the border officials do not have the machines to read the cards and do not know when they will get them. They should be bought and the law enforced without further delay.

THE SOLUTION: ALIEN ID CARDS

We are not going to tolerate a system that treats U.S. citizens and aliens the same; all aliens are not terrorists, but nearly all terrorists are aliens. We do not want to live in a police state, where every American is treated like a terrorist, drug trafficker, money launderer, illegal alien, or common criminal.

Larry Ellison, the head of Oracle Corp., the leading database software company, has offered to donate the tools for creating machine-readable ID cards that contain digitized thumbprints and photographs. A government ID card requirement would allow Oracle's government and industry customers to more accurately monitor the citizens in their privacy-invading databases.



11/15/01 THU 13:06 FAX EAGLE FORUM 004

3

We should have a **computerized database of all aliens entering the United States**, whether they are tourists, students, or workers, and a tracking system that flags the file when a visa expires. Aliens should be required to carry smart ID cards that contain biometric identifiers, the terms of their visas, and a record of their border crossings and travels within our country, similar to the rubber stamps used in all passports.

Airports should be equipped with the machines to swipe the smart card every time an alien boards a plane. Dumb questions like "Has your luggage been under your control since you packed it?" should be replaced with useful questions like "Are you a U.S. citizen?".

The Bush Administration has rejected proposals for a national ID card for U.S. citizens and no member of Congress has introduced ID card legislation. Let's keep it that way.

Faithfully,

Phyllis Schlafly